Treball Final de Grau

Guia de bones pràctiques per mantenir la privacitat en un món connectat

Grau en Enginyeria TIC

Curs 18/19

Autor: KHARBOUCH, Hafid

Director: MONCUNILL GENIZ, Francesc Xavier

Data: 11/10/18

Localitat: Manresa

Resum de Projecte

El tema que es tractarà en aquest projecte serà la privacitat en un món connectat, concretament quin és el grau de privacitat ofert pels diferents serveis usats dia a dia. L'anàlisi que és farà es basarà en les característiques de cada servei, així mateix també s'estudiaran les seves polítiques de privacitat i es compararà l'eina analitzada amb els seus alterns. Finalment, l'estudi teòric se sublimarà en una guia que recollirà les millors opcions per cada servei estudiat.

El projecte buscarà trobar les principals característiques que fan a una eina de la xarxa més segura i privada, buscant un marc comú basat en principis com ara l'importància del codi obert o la relació inversa entre seguretat i usabilitat.

L'objectiu de l'escrit és dotar al lector d'un nou marc de referència a l'hora de decidir quins serveis poden ser més favorables o no respecte seu dret d'anonimat, així mateix el document també busca desenvolupar el sentit crític dels usuaris i instar a què aquests qüestionin els serveis que no fan un ús responsable de la seva informació.

Resumen de proyecto

El tema que trataremos en este proyecto sera la privacidad en un mundo conectado, concretamente cual es el grado de privacidad ofertado por los diferentes servicios usados día a día. El análisis que se hará se basara en las características de cada servicio, asi mismo también se estudiaran sus políticas de privacidad y se comparara la herramienta analizada con sus alternos. Finalmente, el estudio teórico se sublimara en una guía que recogerá las mejores opciones para cada servicio estudiado.

El proyecto buscara encontrar las principales características que hacen a una herramienta de la red más segura i privada, buscando un marco común basado en principios como la importancia del código libre o la relación inversa entre seguridad i usabilidad.

El objetivo del escrito es dotar al lector de un nuevo marco de referencia a la hora de decidir que servicios pueden ser más favorables o no respecto a su derecho al anonimato, así mismo el documento también buscara desarrollar el sentido critico de los usuarios e instar a que estos cuestionen los servicios que no hacen un uso responsable de su información.

Abstract

The topic we will study in this project will be privacy in a connected world, more specifically what is the degree of privacy offered by the different services used every day. The analysis that will be made will be based on the charecteristics of each service, as well we will study their privacy policies and we will compare each analyzed tool with its alternatives. Finally, the theorical study will be sublimed into a guide that will collect the best options for each service studied.

The project will seek the main charecteristics that make an Internet tool more secure and private, looking form a common framework based on principles such as the importance of free code or the inverse relationship between security and usability

The goal of the project is to give the reader with a new frame of reference when deciding which services may be more favorable or not according their right to anonimity, likewise the document will also seek to develop the critical sense of the users and urge that they question the services that do not make a responsible use of their information

Contents

1 Introducció

El tema d'estudi elegit per aquest projecte és estudiar la privacitat en un món connectat. El motiu de per què s'ha elegit aquest tema és a causa del desinterès generalitzat per part de la immensa majoria d'usuaris en aspectes de privacitat, sovint enfocat amb idees nocives com "No tinc res a amagar" o "Encara que m'amagui, acabaran sabent-t'ho tot". El benefici pràctic d'aquest treball és donar visibilitat a un seguit de problemes i situacions de les quals els usuaris no en són conscients o simplement ignoren activament. Donar visibilitat al problema és el primer pas per trobar la solució. Aquest estudi adquireix rellevància en estar cada cop en un món més entrellaçat amb les xarxes, on la nostra informació comença a tenir més d'un propietari. La privacitat és una qüestió de poder, la nostra informació i els nostres secrets poden condicionar-nos com a individus i si, donat el cas, un tercer es fes amb aquesta informació, aquest tindria poder sobre nosaltres.

Per fer-nos una idea, podem utilitzar l'analogia del carter, en la vida quotidiana en enviar una carta som conscients que abans d'arribar al nostre destinatari passarà per l'oficina de correus i serà transportada en determinades condicions, així mateix, si traslladem aquesta situació a la web tenim un canvi radical, passem a tenir centenars d'intermediaris entre nosaltres i el nostre destinatari i gairebé sempre les cartes li arribaran al receptor obertes, amb el contingut copiat en algun dels molts nodes per als quals ha passat. Tot això sense el nostre consentiment i en molts casos, sense el nostre coneixement.

La metodologia que se seguirà consistirà a fer una anàlisi de les diferents eines i aplicacions més usades i un cop haguí determinat els seus pros i contres, es farà una guia d'ús per tal d'incrementar la protecció. Dividirem aquestes eines en blocs més generalitzats de les capes més baixes d'Internet a les més altes, començant per un estudi del Hardware i les seves implicacions en la privacitat, seguit de la importància capital dels sistemes operatius, també estudiarem el paper clau que juguen les xarxes de navegació en l'intercanvi d'informació. En l'àmbit d'aplicació, compararem els diferents navegadors més utilitzats i els seus respectius cercadors d'informació. Finalment es farà una repassada als sistemes de missatgeria web i mòbil, donant una breu ullada també a les xarxes socials i el perill inherent que tenen aquestes sobre la privacitat.

Finalitzat l'estudi teòric, la part practica consistira en una síntesi de l'escrit per determinar quines són les millors eines i configuracions per tal que la nostra informació estigui més protegida. L'objectiu un cop complert, li donarà al lector una nova visió i perspectiva de fins a quin punt és d'important la privacitat, dotant-lo de les eines més recomanades per complir amb aquesta fita.

2 Dret a la privacitat

Entenem com a privacitat a la xarxa com aquell conjunt de factors, eines i practiques que protegeixen la nostra informació, sigui en forma de les comunicacions o la mateixa informació en si. Les principals amenaces que sorgeixen d'una pèrdua de privacitat poden variar des del robatori de dades importants com ara números d'identitat o bancaris fins a monitoratge de l'activitat de l'usuari. Una privacitat assegurada ens ofereix seguretat en navegar per la xarxa mentre que una falta total d'aquesta ens situa en una posició d'indefensió, ja que l'entitat que controla les nostres dades personals pot exercir poder sobre nosaltres. Al llarg del temps la definició de privacitat a la xarxa ha anat mutant, inicialment es podia considerar que no recollir cap mena d'informació de l'usuari era acceptable, actualment es pot considerar que un servei ofereix un nivell moderat de privacitat quan aquest al recollir aquesta informació s'assegura que no pot comprometre la identitat de l'usuari.

Considerarem el dret a la privacitat com aquell dret que ens permet navegar per la xarxa sense haver de preocupar-nos pels problemes anteriorment esmentats. Tot i que en l'àmbit legislatiu això està ben regulat, quan tenim les xarxes pel mig aquesta definició perd contrast. On està el dret a la privacitat? En l'àmbit legal això és subjectiu, com més seguretat i control ens ofereix un servei, més llibertats perdem com a usuaris. A la inversa, com més mesures busquem nosaltres per a protegir-nos més sortim perdent sigui per pèrdua d'usabilitat o la inversió de recursos que suposa haver d'estar atent a com d'invasiu és un determinat servei, trobant-nos en una situació d'indefensió per les dues bandes La nostra activitat a la xarxa és com un cotxe deixant informació per un tub d'escapament, informació que s'utilitza sense el nostre consentiment o coneixement. En aquest cas tota la informació que generem com a consumidors d'informació és un actiu que té un valor determinat, d'aquesta manera, al no tenir que pagar per un servei com és Internet (en el sentit estricte de la paraula) el producte passem a ser nosaltres, o més ben dit, la nostra activitat.

Una possible solució per això és eliminar el nombre d'intermediaris i reduir-ho tot a connexions directes, per exemple, [12] Facebook en aquest cas (tot i les seves deficiències que contemplarem) junta individus que busquen contingut multimèdia amb gent que els genera, limitant la quantitat de persones i serveis que estan pel mig. Google ofereix una opció d'intermediari innecessària, cada cop que fem una cerca per al seu buscador i volem entrar a un dels enllaços resultants, el que fem realment és passar per una pàgina intermediaria de Google que enregistra quin és l'enllaç al qual hem accedit.

La seguretat és un procés i un seguit d'actituds que cada individu ajusta a la seva manera, per molt bones eines que tinguem de cara a la protecció, aquestes són inútils si el compartim informació sensible per canals públics o si entrem en serveis que ja tenen una fama qüestionable. Així mateix, hem vist que els sistemes operatius juguen un paper clau en la protecció de cara cap endins, així i tot

Internet es basa en les connexions i comunicacions cap a l'exterior i la primera capa que es troba entre la comunicació dels nostres dispositius és la de xarxa, protegir aquesta capa adquireix una prioritat similar a la del sistema operatiu com que tot el que fem a Internet requereix una xarxa que ho sustenti i que ofereixi uns mínims de seguretat.

3 Hardware

Abans d'adentrar-nos en el món dels sistemes operatius, farem un breu incís en la importància del hardware. Sota de totes les capes d'aplicació i sistemes operatius, sempre tindrem el hardware en la més profunda de totes. És d'imperativa importància recordar que tota la seguretat i totes les proteccions que comentarem convertiran en paper mullat en el precís instant en què algú tingui accés físic al dispositiu que volem protegir, sigui l'ordinador, mòbil o encaminador.

Per exemplificar podem agafar el cas més bàsic que seria el d'un keylogger en el teclat, un dispositiu que enregistra tot el que escrivim. El problema aquí no rau en el microprocessador del teclat si no cap on surt el cable d'aquest, un keylogger d'aquestes característiques pot conec-tar per un punt al teclat i per l'altre a l'ordinador, convertint-lo en una eina discreta. Sense ficar-nos amb hardware dissenyat exclusivament en segrestar informació, també podem parlar del perill que suposen els teclats inalambrics, ja que aquests retransmetrien el seva senyal a qualsevol dispositiu que pugi escoltar en el seu rang, el grau d'encriptació d'aquesta informació pot variar depenent del model i l'antiguitat.

Deixant de banda la discreció d'aquests petits malwares, també entren en escena els discs durs dels ordinadors, avui en dia la tecnologia dels discs durs HDD està quedant essent avançada pels nous discs durs SDD, que a part de ser més durables també ofereixen un graó en velocitat que els fa més interessants que els HDD. Al tractar-se de dues tecnologies diferents, moltes possibilitats d'eliminació total de dades no estan a l'abast en memòries SSD, en les memòries HDD, quan escrivim sobre aquestes el que estem fent és ficar un seguit d'uns o zeros en una determinada taula del disc magnètic, per esborrar la informació d'aquests, només hem de sobreescriure múltiples vegades sobre la mateixa taula per tal de borar-ho, per altra banda, una SSD és un laberint de semiconductors que fan un emmagatzemat diferent, provocant que un cop aquestes memòries estan essent utilitzades per un sistema operatiu, quan aquest esborra taules de memòria únicament les està marcant com a zones de memòria invalides, ja que el fet de setejar a 0 taules de memòria és costós en l'àmbit de recursos, això ens deixa en una situació en la qual inclòs després d'esborrar un fitxer del nostre sistema realment no sabem si ha desaparegut per sempre.

Per al que fa el hardware de la xarxa, Internet en sí, les nostres preocupacions han d'esser limitades, ja que el disseny per capes més baixes de la xarxa (física i d'enllaç) són benèvoles de per sí, limitant-se únicament al transport de dades sense fer judicis del contingut d'aquestes, de manera que ens hem de preocupar de les capes de més dalt, ja que aquestes són les que poden ocasionar forats en la nostra privacitat (siguin les capes de xarxa o les mateixes aplicacions). A part d'aquests breus incisos, un hardware que mai sigui manipulat per tercers és un hardware segur, de manera que podem continuar al següent nivell, la capa que tenim per sobre és la dels sistemes operatius.

4 Sistemes operatius

A una capa més baixa de la seguretat de les nostres dades, entren en joc els sistemes operatius sobre els quals portarem a terme totes les nostres activitats. Quan qualsevol aplicació del sistema vol fer alguna acció (llegir informació, conectar-se a Internet) ho fa a través del SO, ficant en aquest en una posició on absolutament tot el que passa dintre del sistema està a la seva vista.

Hem de fer l'incís en què això no és singular en alguns determinants sistemes sinó que **tot sistema operatiu per disseny té aquest nivell d'observació en les nostres accions**, per tant, similar al punt de les encriptacions de servidor, el saber que està fent amb la nostra informació el sistema es redueix a una qüestió de confiança, molt similar al que havíem plantejat en l'apartat de serveis Google.

Enfocarem aquest estudi des de dos vessants, des de la mòbil i la d'ordinador de sobretaula. Per una banda tindrem els sistemes operatius enfocats a ordinadors, tals com Microsoft Windows, MacOS i GUN/Linux (essent els més populars en aquest ordre), per l'altra, tindrem els de telèfons mòbils: Android, IOS (Iphone OS), Microsoft WindowsPhone i altres no tan utilitzats

4.1 Microsoft Windows

Com ja hem vist anteriorment, la política de Microsoft Windows insta a oferir a l'usuari un control, transparència i seguretat sobre les seves dades, fent menció a la generació d'anuncis a partir de la identificació de l'usuari recopilada del propietari.

Així mateix, podem veure que es repeteix la filosofia d'alguns navegadors que ja hem vist: S'utilitza la informació recopilada per a generar millors resultats, cosa que pot acabar provocant un filtre bombolla a la llarga. Com a altres característiques aquesta decisió es opcional i la podem deshabilitar des-de la configuració [1]. Una altra característica deshabilitable és la d'informació d'ubicació, que determina la nostra posició a partir de les adreces IP a les que ens connectem.

Figure 1: Logotip Microsoft Windows

A causa de les diferents distribucions de Microsoft Windows, ens centrarem en la més actual: Microsoft Windows 10. Aquesta comença amb punts importants com el tractament de la informació personal durant s'insta-la un nou programa al sistema com ara informació del dispositiu i de les aplicacions que aquest te registrades. També queden recopilades les dades de veu enregistrades en el sistema -per exemple, si una aplicació té funcionalitat de veu, Microsoft Windows recopila qualsevol enregistrament i l'utilitza com a mostra per poder millorar les seves funcionalitats de processament de

la parla-.

Aquesta política agressiva va un pas més enllà quan podem veure que també es registren les dades dels fitxers que obrim (quin tipus de fitxer era, amb quina aplicació es va obrir...) o quins són els caràcters teclejats, tot això amb el pretext de què són mostres per tal de millorar el sistema operatiu. Tot i que Microsoft ens avisa de tots aquests aspectes en la seva política de privacitat trobada durant l'instal·lació, no deixa de ser una recopilació de dades agressiva.

When people choose to turn on location services, we get to improve our location services by collecting information about the location of mobile phone masts and WiFi access points. This information is stored in a database without data identifying the person or device from which it was collected.

If you turn on **Speech, inking & typing**, we collect samples of your typing and handwriting info to improve our dictionaries and handwriting recognition for everybody who uses Windows. We take care to remove identifiers and store the data chopped up into small, random chunks so that we can use the information for product improvement while protecting the identities of users who submitted it.

Figure 2: Extracte de la política de privacitat de Microsoft Windows

S'ha d'afegir també el fet que les actualitzacions passen a ser obligatòries a Microsoft Windows 10, això vol dir que el sistema pot actualitzar qualsevol aplicació ja instal·lada sense avisar-nos prèviament ni demanant-nos el consentiment. De manera que nosaltres com a usuaris no podem tenir control sobre que entra i que surt del nostre ordinador, relegant el nostre paper a observador i no propietari [5]

Així mateix, arribem a un punt d'inflexió, per una banda podem evitar tota aquesta recopilació utilitzant versions de Microsoft Windows o bé modificades amb determinats propòsits o bé ja dissenyades des de el principi per la pròpia Microsoft per evitar fuga de dades (tals com Microsoft Windows entreprise edition, que prohibeix la transmissió de dades als servidors d'aquesta). Veient les alternatives, l'opció d'un altre sistema operatiu és més cridanera donat que la quantitat d'informació recopilada amb la qual ens trobem aquí és massa elevada.

4.2 MacOS

De nou, ens trobem en una situació en la qual es fa una recopilació anonimitzada per tal de tenir mostres però no poder determinar el propietari d'aquestes [2], Apple s'excusa amb la mateixa idea que els altres sistemes operatius: Per tal de millorar els seus serveis. Tot i que tenim moltes opcions per tal de determinar quina informació s'envia a serveis Apple i quina no, de poc ens serveix activar o desactivar funcionalitats si a una escala major l'arquitectura del sistema tremola a tots els nivells.

Figure 3: Logotip Mac/IOS

Ens podem trobar en situacions complexes com ara que el mateix sistema operatiu decideixi que no vol actualitzar una aplicació, aquest va ser el cas amb

Telegram durant quan aquest va ser censurat i bloquejat en Rússia [9], això va implicar que l'aplicació no es pogués actualitzar arreu del món a causa de la pressió d'un país a l'empresa, situacions com aquesta ens fan desconfiar del grau de benevolència que pot tenir un sistema operatiu amb l'usuari.

Intrusions més extremes serien com les de la distribució de Mac High Sierra, que actuava directament sobre el hardware del disc dur, obligant a la memòria SSD a APFS(APple File System) [8], provocant que un cop canviada l'estructura de fitxers del disc, aquests fossin irreconciliables per altres sistemes operatius, obligant a formatejar la partició.

Són notícies com aquestes les que ens fan arribar a la conclusió de què no només necessitem unes opcions sòlides per protegir la nostra informació, sinó que la nostra pròpia experiència d'usuari ha d'estar lliure D'Interferències externes per part del sistema operatiu. Un cop comprat un Software o Hardware, aquest passa a ser propietat nostra indefinidament, que el sistema operatiu moderi aquesta propietat arbitràriament és inacceptable.

4.3 GNU/Linux

Tractant-se del sistema operatiu de codi obert més conegut i utilitzat, conceptes com la seguretat o protecció de dades vénen ja donats, així i tot, farem la repassada obligatòria a les bases de la seva política de privacitat [3]. Com hem vist a moltes altres polítiques, es recull determinada informació personal a canvi d'oferir certes característiques o la participació en alguns aspectes dels diferents projectes oberts de GNU/Linux.

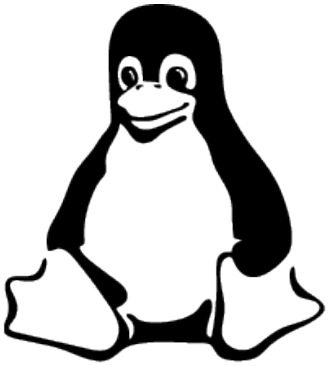


Figure 4: Logotip GNU/Linux

Un dels principals avantatges que trobem de GNU/Linux és la possibilitat de crear diferents distribucions depenent de les nostres necessitats, això ens obre un extens ventall en diferents sistemes operatius basats en GNU/Linux que estan centrats únicament en la privacitat [4], tot això és gràcies a les seves característiques de codi obert (També ens podem trobar amb distribucions que natives de GNU/Linux que no ens protegeixen, com ara Chrome OS i Android). Tampoc hem de caure en el parany de pensar que un cop estem utilitzant aquest sistema operatiu quedem lliures de tots els mals, la seguretat és un procés constant.

D'entre les moltes bones pràctiques que podem dur a terme encriptar el disc dur és una de les més recomanables, ja que ens permet tenir tot el directori principal protegit en tot moment amb una capa afegida de seguretat. Per a usuaris més avançats, GNU/Linux pot suposar una eina molt favorable a causa de la llibertat d'ús que ofereix

la seva terminal, podent arribar a utilitzar comandes que ens permeten veure els serveis que estan actius en determinats ports de sortida del nostre ordinador.

Un dels beneficis de tenir una base d'usuaris tan petita a GNU/Linux (un 1.5% comparat amb el 83% de Microsoft Windows en l'àmbit mundial[**?**] és que els creadors de Malware preferiran tenir com a target una base més gran i vulnerable, en aquest cas Microsoft Windows. Una comunitat petita com la de GNU/Linux (i de codi obert) també permet l'evolució del sistema gràcies a què els mateixos usuaris poden proposar i implementar canvis en les seves pròpies distribucions o fins i tot, amb esforç, tenir millores acceptades per part del Kernel de GNU/Linux.

Com sempre, en la protecció de la privacitat la proactivitat de l'usuari juga un paper important com que encara que el nostre sistema sigui inexpugnable, són les nostres accions com a usuaris les que ens poden ficar en perill determinats cops. Tampoc hem d'oblidar que la seguretat d'un sistema no està relacionada amb la privacitat d'aquest, és a dir, per molt segur que pugui ser GNU/Linux, aquest no podrà fer res per protegir-nos en el cas que enviem dades sensibles per correu electrònic.

La seva estructura de sistemes d'usuaris també permet un ús responsable en aquells sistemes on no només treballem amb un usuari, l'administrador pot permetre a diferents usuaris alguns permisos determinats, ja sigui només poder visualitzar documents, editar-los o fins i tot executar-los.

Podem determinar que GNU/Linux ofereix uns nivells de privacitat més que acceptables, amb la possibilitat d'incrementar aquests nivells amb les seves múltiples distribucions. Així mateix, per mantenir balancejats els nivells de privacitat amb els d'usabilitat, una distribució simple de GNU/Linux (per exemple Ubuntu) pot ser més que suficient per a les nostres necessitats.

4.4 Altres

Depenen del tipus d'usuari que siguem i fins a quin punt volem protegir la nostra privacitat, els sistemes operatius convencionals se'ns poden quedar curts, per això disposem d'alternatives extremes tals com sistemes operatius dissenyats amb un clar objectiu en ment, una de les alternatives disponibles és Tails (The Amnesic Incognito Live System),

Una de les seves principals fortaleses és el fet que en cap moment el sistema operatiu toca el disc dur, això ofereix dos beneficis: Primerament, el sistema operatiu no deixa cap traça sobre una memòria que pot ser analitzada per un individu aliè, i segon, ens ofereix la seguretat de no estar pendents de si el software instal·lat decideix indagar en informació altament sensible (que communment enregistrarem al disc dur). Un altre punt atractiu de Tails és que el tràfic de xarxa ens ve ja encaminat per Tor, que tal com ja havíem comentat, sol ser una de les fortaleses més difícils de penetrar per al que seguretat comporta.

A nivell d'usabilitat és força amigable, ja que totes les eines que necessitem ja ens venen pre-

instal·lades i pre-configurades.

Així mateix, podem veure que la millor alternativa de la qual disposem en l'àmbit de sistemes operatius de sobretaula és la de tenir un liveCd amb Tails ja instal·lat. D'altra banda, qualsevol distribució de GNU/Linux ens pot oferir uns mínims acceptables, mínims que no superen els anteriors sistemes ja esmentats.

5 Sistemes operatius mòbils

Per al que fa els telèfons mòbils, ens trobem amb uns dispositius que per naturalesa ja delaten moltíssima informació sense que nosaltres puguem fer gaire. Com que la primera capa de seguretat d'un telèfon és el mateix sistema operatiu anem a fer un repàs als diferents sistemes mòbils dels quals disposem.

5.1 Android

Android és un sistema operatiu desenvolupat per Google de la família de sistemes Unix, per al que fa la seva popularitat, des del 2011 ha sigut líder indiscutible en sistema operatiu mòbil més vengut. Dintre d'Android com a tal també trobem associat diferent software de Google que ve a ser el conjunt d'aplicacions que ja ens vénen donades al nucli del sistema. Com ja vàrem abordar en serveis Google, tot el que respecte a Android està fortament lligat a la telemetria utilitzada per dotar d'un control total als serveis Google, no ens fa falta investigar més enllà per determinar que Android no és una bona opció per protegir la nostra privacitat.

Arribem a la conclusió següent: Els serveis Google instal·lats en Android són altament invasius i tot i evitar-los podem trobar-nos amb què la telemetria de Google segueix sobre nostre. Una alternativa pot ser utilitzar sistemes Android personalitzats per evitar aquests inconvenients, tot i així'ns en ser productes manufacturats per particulars no podem confiar en la seva total funcionalitat i hem d'acceptar una certa limitació en les seves capacitats, això també comporta un gran inconvenient i és que per instal·lar aquests sistemes modificats hem de ser root en el telèfon, cosa que pot provocar situacions de vulnerabilitat, ja que a l'obrir totes les portes del sistema perquè siguem administradors també ens exposem a nous perills que abans ja estaven resolts pel sistema operatiu. De totes maneres i veient les alternatives, potser Android és el mal menor.

Figure 5: Logotip Android

5.2 IOS

IoS és el sistema que es ve donat per defecte en les distribucions mòbil de Mac, en tot Iphone/Ipad trobarem una versió diferent del sistema operatiu. Dels diferents paràmetres de privacitat que podem controlar tenim per exemple el tracking de geo localització, que ens permet decidir quines aplicacions poden monitoritzar la nostra posició i en el millor dels casos, determinar que cap ho faci. Per al que

fa la navegació, tenim la possibilitat de dir-li al navegador per defecte (Safari en aquest cas) que activi certes característiques com el bloqueig de pop-ups i el monitoratge de webs sobre l'usuari

Tot i que la cosa es complica quan queda confirmat que Apple te la capacitat d'eliminar aplicacions del nostre Iphone en considerar-les inapropiades [7], tot i que l'existència d'aquesta funcionalitat ha quedat demostrada i admesa per la pròpia Apple, encara no s'han donat casos de desinstal·lacions a distància d'aplicacions d'usuaris. Tot i que aquest fet es va demostrar fa anys, el dia d'avui no podem determinar si aquesta funcionalitat segueix vigent als nous models, tot i així, tenir una porta posterior dissenyada per aquests fins a ja fa saltar alarmes respecte al control que Apple manté sobre l'usuari.

Un dels casos més preocupants és la propietat del hardware de l'Iphone, tècnicament és de l'usuari, de voler fer reparacions en el dispositiu (com ara el botó central de home), de no fer-ho en una distribuïdora oficial d'Apple serem víctimes d'un bloqueig de software, de manera que les característiques d'identificació per tacte o simplement tornar a la vista de Home queden bloquejades [10].

5.3 WindowsPhone

Microsoft WindowsPhone no ofereix diferències notables comparat amb els seus alterns, seguint una política de privacitat idèntica a la de Microsoft Windows, ens trobem amb un sistema que requereix un feedback constant de l'usuari, feedback que es converteix ràpidament en monitoratge d'aquest. Ens trobem de nou amb situacions similars a les de Ios, on el distribuïdor determina que podem i que no instal·lar, amb situacions en les quals de voler instal·lar un altre sistema operatiu sobre el dispositiu que porta Microsoft Windows de sèrie es compliquen de sobremanera arribant a casos de bloqueig de dispositiu [11].

6 Xarxes

En voler utilitzar una xarxa segura, la majora de les necessitats [16] dels usuaris es redueixen en tres demandes:

- Saltejar la censura web
- Entrar a webs amb restriccions geogràfiques
- Millorar la seguretat a Internet

D'aquesta manera, estudiarem a tres eines [17] que busquen cobrir aquests tres punts.

6.1 Xarxa d'anonimat TOR

De naturalesa lliure, aquest programari permet navegar anònimament per la xarxa de manera que encamina els paquets per una xarxa voluntària que oculta la identitat, ubicació i trafic que generem per evitar la vigilància o monitoratge de tercers [13]. Això solucionaria gran part dels nostres problemes que hem anat veient en els navegadors i cercadors, tot i així es una arma de doble fil ja que pot dificultar les visites i l'enviament de missatges, per no entrar en el fet de que es la principal porta a Internet per a les activitats il·lícites, de manera que només entrar-hi ja pot ser considerat una actitud sospitosa de cara als serveis de intel·ligència.

Se'l coneix com encaminament de ceba perquè la seva encriptació és similar a les capes d'una ceba, encripta les nostres dades diverses vegades i les envia per un circuit de nodes creat a l'atzar de manera que cada parada (cada node) desencripta una petita part de la capa, el node final rep les dades sense saber qui ha fet la petició inicial. Per tal de mantenir una comunicació dinàmica i dificultar un anàlisi de les nostres comunicacions, cada 10 minuts els nodes de connexió Tor que tenim van canviant [14]. En ser una xarxa pública, si ens convertim en un node incrementem la privacitat de la xarxa

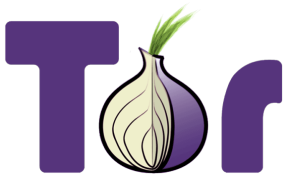


Figure 6: Logotip Tor Project

Això fa que qualsevol tercer en cerca de la nostra informació ho tingui molt més complicat per a accedir a les nostres dades. És important repetir que gràcies a Tor **tots els nodes intermitjos no saben d'on ve ni cap a on va la nostra informació**. Com qualsevol sistema tecnològic, no és infal·lible, però així i tot és una millora de la situació inicial. Així i tot estem lluny de la promesa de privacitat total, com ja hem comentat ser usuari de Tor ja et fica en un cert perfil d'usuari que és més fàcil de ser apuntat per agències d'intel·ligència nacional [15].

L'anonimat tampoc es pot relacionar directament amb la seguretat, ja que el navegador també pot ser una porta a tercers individus, essent molt més fàcil així que colar-se en la xarxa directament. Un "Man in the midle" segueix sent possible a Tor. En paraules dels seus creadors "Tor no és suficient per mantenir-te segur la majoria dels casos". Tor serà tan útil com ho sigui el nostre navegador, si aquest últim està blindat i és segur, utilitzar la xarxa Tor serà més efectiva.

6.2 VPN

L'alternativa elegant i simple a una xarxa Tor pot esser una VPN. Una VPN es una xarxa privada virtual, tot i que el seu us pot estar relacionat amb el treball amb xarxes privades de empreses, ens centrarem en la part d'usuari de a carrer i com aquesta por ajudar a incrementar la seva privacitat [19].

Es un servei que una vegada contractat està actiu cada vegada que estem en linina, en termes generals manté el anonimat i ens permet l'accés a llocs censurats, la xarxa VPN ens ofereix una IP temporal que amaga la nostra IP real que s'utilitza en la majora de serveis online. Ja que la IP queda maquillada, aquesta no es pot vincular al nostre dispositiu, això permet que el nostre proveïdor de internet i tercers usuaris no sàpiguen on hem estat. A més a més, la connexió està xifrada, evitant una fuga de informació i de haver-ni, essent completament illegible.

Podríem entendre aquest tipus de xarxa com a un sistema que permet connectar-nos a una red publica com si estiguéssim connectats a una xarxa privada de casa o de la empresa.

6.3 Proxy

Un proxy es un ordinador que canalitza la nostra connexió de manera que actua com a una capa extra entre el nostre dispositiu i Internet, el resultat es que de cara a Internet, qui està connectat es el proxy i no nosaltres, fent de substitut. En tenim de dos tipus:

- Http: Són simples i permeten canalitzar tràfic de les pàgines web, tenen un ocultament d'IP ineficient i només serveixen per navegar
- Socks: No interpreten el tràfic i poden filtrar qualsevol tipus d'informació que nosaltres li diguem.

Com ja hem dit, un proxy és un ordinador que reencamina la nostra activitat web, quan fem una petició web aquesta va ael nostre proveïdor però just després és reencamina cap al proxy i d'allà cap a la destinació final que buscàvem, el camí de tornada dels paquets és el mateix per a la inversa. Dintre de les opcions que hem barallat aquesta pot ser la que requereix menys simplicitat tècnica, ja que es poden trobar diferents serveis proxy gratuïts a la xarxa, així i tot tenim riscos [18].

Suposem que tenim un servei Proxy contractat i enviem un missatge, primer de tot, el nostre missatge ha de passar per al servidor proxy abans d'arribar al destí i sense encriptar, essent un blanc fàcil per a qualsevol tercer o inclòs el propietari del proxy, fent-lo el man in the middle perfecte. L'única manera de poder passar per alt aquests perills és buscar un servidor que tingui la nostra confiança total.

6.4 Comparativa

Primerament tenim a Tor amagant la nostra IP i fent salts aleatoris entre els nodes, fent molt difícil de seguir la traça que deixem, així i tot d'arribar al últim node i tenir el paquet desprotegit (com que el lloc no és segur) aquest pot córrer perill, i amb ell la informació que enviem. També hem de tenir en compte que a causa dels múltiples salts, inevitablement la velocitat de connexió es veurà reduïda. Com ja hem comentat anteriorment, com que la xarxa Tor és utilitzada majoritàriament per individus susceptibles a ser monitoritzats degut a les seves activitats, nosaltres també podríem caure en la motorització d'una agència d'intel·ligència. Com a últim detall podem ultimar que és molt recomanable per a activitats que requereixen especial anonimat.

A una VPN no fem tants salts, ja que la nostra connexió és un tunel que va directe cap a la web que hem demanat, eliminant la possibilitat de trobar-nos amb un Man in the middle. Una problemàtica que pot sorgir és que escollim un servei VPN que registri la informació que circula per ell, fent-la sensible a una petició legal, també és important que el servidor de VPN pugui repartir la seva càrrega de peticions i que els diferents usuaris vaguin canviant de servidors vpn. En definitiva, recomanable per anonimat a la web, així i tot és un servei de pagament.

Qualitats	PROXY	VPN	TOR
Velocitat	Al només requerir HTTP requests, la velocitat queda agilitzada	Generalment ràpid,tot i així els serveisgratuïts poden ser lents	Extremadament lent
Privacitat	El tràfic no està encriptat	Connexió encriptada i privada, tot i així el proveïdor pot saber que estem fent	Ofereix un anonimat total,la connexió està encriptadaa múltiples capes
Preu	Tenim varietat d'opcions i acostumen a ser barats	A més fiabilitat demanada, més alt pot ser el preu del servei	Gratuït
Seguretat	Els Proxy gratuïts són un perill per a la seguretat	Actuen com a un tunel cap a la nostra connexió, fent-los segurs de cara a un "Man in the middle"	La informació saltaentre diferents nodes.Tot i així pot ser perillósinclòs sense fer res il·legal
Usabilitat	S'ha de configurar cada servei individualment(correu, navegador, ...)	En ser un servei de pagament, el proveïdor ja s'ocupa de simplificar la nostra feina	Permet l'accés a la deep web, però requereix l'aprenentatge de certes eines i tenir un coneixement avançat en xarxes

Figure 7: Comparativa entre eines de privacitat

Proxy per altra banda tendeix a la simplicitat màxima, afegint una única capa sobre la nostra connexió que en aquest cas és un altre ordinador. La majoria de proxys no està dissenyat per protegir el nostre tràfic, de manera que molts proxy envien inclòs la nostra IP en fer les peticions web. També hem de tenir en compte el fet que s'han de configurar individualment per cada aplicació que tingui accés a la xarxa i moltes webs i serveis d'internet no permeten l'accés si detecten que un proxy els hi estan demanant informació. Pocs són els beneficis que té a diferència del VPN que el supera en gairebé tots dels seus apartats, podríem utilitzar un Proxy per a recomanable per accedir una pàgina particular està bloquejada pel teu ISP

La conclusió és que per cada activitat que vulguem fer, una eina seria més útil que l'altre (mirar vídeos, mail, jugar, entrar en webs anònimament...), Proxy és una solució limitada que es queda curta per a les necessitats bàsiques i inclòs alguns poden fer més mal que ve ficant-nos en perill. Tor és una solució flexible i gratuïta, però amb els seus inconvenients propis.

Per a busqueres del dia a dia, el veredicte seria contractar una xarxa VPN. De voler tenir una privacitat total, la combinació de Tor i xarxa VPN ens pot blindar molt de tercers observadors.

7 Navegadors

Un navegador web (entenent-lo com a un software que permet l'accés a un servei http) serveix per visualitzar documents ubicats en altres ordinadors, aquesta transmissió dels documents és gràcies a Internet. Així mateix, deixant de banda tots els beneficis que comporta utilitzar un navegador web, tots els navegadors fan ús de la informació que reben de nosaltres sense que en siguem completament, ens centrarem a determinar quines polítiques de privacitat tenen i encara més important: Que signifiquen per a nosaltres, els usuaris.

7.1 Mozilla Firefox

Mozilla Firefox fa la distinció entre informació personal i no personal, essent la de caràcter personal aquella que identifica a l'usuari, nom o mail. Qualsevol tipus d'informació que rebi Mozilla Firefox passarà a ser personal en el moment en què estigui combinada amb parts d'informació personal.

El navegador de Firefox obté informació dels usuaris de les següents maneres:

- Subministrades per el mateix usuari - enviament d'informes de fallida
- A través dels productes i serveis - Quan l'aplicació verifica si està actualitzada
- A traves de tercers - Thunderbird
- Amb informació ja proporcionada - Adaptar l'idioma a través de la IP

Figure 8: Logotip Mozilla firefox

És interessant anotar que Mozilla Firefox només utilitzarà la informació personal en finalitats que hàgem permès nosaltres. Així doncs, hem de fer una anàlisi en quines situacions MozillaFirefox comparteix la nostra informació amb tercers. Primerament ho farà en el cas que tingui el nostre permís per fer-ho, també es podrà donar aquesta informació a tercers per tal de millorar al servei, amb la clàusula que aquests tractaran les dades d'acord amb les directives de Mozilla, tot això ve lligat amb la missió de transparència de Mozilla Firefox [20] on *"Eventualment es divulgarà informació per millorar els nostres productes i promoure una Internet oberta, però quan ho fem excloem les seves informacions personals per tal de minimitzar el risc d'identificació dels usuaris"*. [21].

Mozilla Firefox també es reserva el dret de cedir la nostra informació quan hi hagui una exigència de la llei, sigui per part de un govern o una acció judicial. Finalment, d'arribar a haver-hi una re-estructuració o successor de l'empresa, aquesta adquiriria la nostra informació també, és a dir **la nostra informació pot seguir tenint una empremta digital) encara que Mozilla passi a ser propietat d'una empresa afiliada**

En el cas de la protecció d'informació, Mozilla Firefox es compromet a avisar-nos en qualsevol violació de la seguretat, a part d'eliminar-la una vegada superat cert temps, la nostra informació és eliminada. Mozilla Firefox també assegura de no voler mantenir informació de menors a 13 anys en cap de les seves bases de dades.

Ara bé, en el cas que aquestes polítiques de privacitat siguin alterades, Mozilla Firefox s'ocuparà d'avisar-nos de quins són els canvis significatius. De seguir utilitzant el producte sense estar conforme amb els canvis, Mozilla Firefox utilitza l'argument de què una vegada passat cert temps, el client està d'acord amb els canvis una vegada ha començat la data en vigor de l'actualització

Respecte a les possibilitats de sincronitzar la informació entre els diferents dispositius que utilitzin la mateixa conta Mozilla [22], la informació que es guarda és la de contrasenyes, pestanyes preferides i configuració. Al borar la conta Mozilla Firefox també s'eliminara aquesta informació.

Afegir que el mode de navegació privada és una de les característiques que ofereixen seguretat en el navegador, anem a veure què ofereix. Principalment aquest mode no emmagatzema les pàgines visitades a l'historial de Mozilla Firefox, així i tot, això no implica que tinguem un anonimat total [23], la navegació privada no protegeix contra cap classe de programari maliciós que pugui rastrejar la nostra activitat, no Keylogers ni programes espia.

7.2 Google Chrome

Google Chrome segueix la política de privacitat de Google. Similar a Mozilla Firefox, al registrar una compta aquesta servira com a font de informació per a Google que aquest utilitzara per mostrar resultats de cerca i anuncis més rellevants d'acord amb el nostre historial [24].

El navegador de Google Chrome obté informació dels usuaris de les següents maneres:

- Subministrades per el propi usuari - enviament de informes de fallida
- A traves dels productes i serveis - Quan l'aplicació verifica si està actualitzada
- A traves de tercers.
- Amb informació ja proporcionada - Adaptar el idioma a traves de la IP
- registre de baixades
- Captures en miniatura de les pagines visitades

Tota aquesta informació s'emmagatzema en l'àmbit local a no ser que estiguem amb la sessió ja iniciada de Google, això implicaria que aquestes dades s'emmagatzamenarien al nuvol en la nostra conta de Google a causa de la funció de sincronització.

Google Chrome també utilitza la renderització prèvia de pàgines per tal de cargarles més ràpidament, això consisteix en què el sistema de busca fa una predicció de quina serà la següent pàgina que demanareu per buscar a partir de les opcions disponibles i les busqueres passades que vàrem fer, tot i no visitar la pàgina renderitzada que Google Chrome creu que visitarem, aquesta llegirà les nostres galetes. Per al que fa la ubicació, almenys Google Chrome no permet que els llocs que visitem tinguin accés a la nostra ubicació a menys que oferim el nostre permís -tot i aixi'ns, en dispositius mòbils aquesta ubicació queda compartida automàticament- . Google Chrome utilitza el servei d'ubicació per a registrar la següent informació:

- Routers més propers
- Identificadors de telefonia mòbil propers
- Intensitat del senyal Wi-fi
- Adreça IP del dispositiu

Figure 9: Logotip Google Chrome

En altres paraules, pot triangular la nostra posició precisa amb tot el que comporta. Seguim indagant en quines utilitats té Google Chrome, com ara la predicció de cerques, quan comencem a fer una cerca a la barra d'adreces de Google Chrome, els caràcters que escrivim -**inclòs aquells que no enviem amb la tecla de retorn** s'envien al motor de cerca i utilitzarà aquelles dades per fer prediccions d'acord ambl nostre historial, als temes relacionats amb la cerca i les peticions de cerca dels altres usuaris.

Per al que fa el mode incògnit, aquest no guarda la informació de l'historial ni el registre de baixades, les galetes creades durant el mode incògnit tenen de data de caducitat fins que se surt de la sessió, per tant deduïm que l'abast d'aquest mode és d'un caire limitat.

7.3 Edge

Microsoft Edge és el navegador per defecte de Windows 10. Primerament al·lega a les bones intencions de la informació recollida, de manera que pot acabar oferint una experiència a mida per cada usuari a mesura que va adquirint informació i cerques d'aquest [25]. En aquest cas Microsoft Edge sí que participa amb altres softwares del sistema, com per exemple l'antivirus de Microsoft "Windows Defender", que determinarà si la pàgina a la que volem accedir és perillosa o sospitosa. Les cookies segueixen igual que en els altres navegadors, només registren configuracions i alguna contrasenya.

Respecte a la declaració de privadesa [26], Microsoft pot compartir la informació que li oferim (i la que extreu de nosaltres) amb les seves filials, amb els treballadors que estan sota ella o per la llei, seguint una filosofia similar a la de Firefox. Així i tot Edge ens permet en gran mesura configurar fins a quin punt pot recollir la nostra informació. Un detall important està en el tractament cap a l'usuari final que fa Edge, en aquest cas, si l'usuari final és un particular treballant per una empresa o una escola, el propietari del domini tindrà accés tota al nostre conte de Microsoft i l'accés a informació i comunicacions que hem tingut, en aquest cas Microsoft al·lega que no és responsabilitat seva.Com a apartat final, recordar que Edge ofereix un serveix per logejarse amb el conte de Microsoft, oferint així'ns una altra via per una fuga d'informació sense que l'usuari en sigui conscient.

7.4 Opera

Opera -amb orígens al 1995- és un navegador que centra els seus esforços en la millora del rendiment, essent un dels seus principals punts forts la gestió de recursos i l'intent en reduir l'ús de bateria en ordinadors portàtils [31]. Per al que fa la personalització del navegador aquest pot compartir extensions amb Google Chrome gràcies a què comparteixen la base amb Chronium. El seu enfocament de configuració segueix la mateixa linneà que havíem vist en anteriors navegadors, centrant-se en un enfocament més estètic (amb alguna configuració per millorar la seguretat) [32].

Des de l'àmbit de privacitat tampoc es queda curt, ja que ens ofereix la possibilitat d'activar una VPN amb els servidors d'Opera, estalviant-nos contractar un servei privat. Totes les altres característiques ofertades no s'escapen gaire de la mitjà que hem anat veient.

Per al que fa la seva política de protecció de dades [33], se centra a explicar que totes les dades recollides per als usuaris se centren a millorar l'experiència oferida i debuggar l'aplicatiu, mencionant en una ocasió la recomanació de publicitat si aquesta és rellevant per a nosaltres - En altres paraules, un intent del navegador per decidir que és el que ens interessa i que no -. Respecte al tipus d'informació recollida, se centren en la metadada del dispositiu que estigui utilitzant Opera (tal com especificacions del hardware). Un dels punts també a comentar és un dels ítems que referència amb qui comparteixen la informació recollida de l'usuari, a part de cossos governamentals que ho demanin i tercers associats a l'empresa, també tindran drets sobre la nostra informació generada aquelles empreses que es facin control de l'empresa original, donant-se una situació en la qual la informació recopilada -per inofensiva que sigui- mai desapareix.

En termes generals la seva política i les funcionalitats oferides no disten gaire de la línia general que hem anat veient dels diferents navegadors, de manera que Opera no acaba destacant ni positivament ni negativament.

7.5 Safari

Safari, navegador web desenvolupat per Apple, es promociona a si mateix com el navegador per defecte dels sistemes Mac i les seves característiques se centren oferir eines per tenir més control (bloqueig total de cookies entre altres) [34]. Tot i així, el fet de compartir política de privacitat amb Apple implica que hi haurà certes maneres de fer que xocaran frontalment amb el nostre objectiu d'una navegació privada. En l'actualitat l'apartat de navegació segura i privada ha sigut un dels principals forts de l'última actualització de Safari [35], amb aquesta millora el navegador adquireix un nou nivell de privacitat, així i tot hi ha dos aspectes que segueixen essent clau per a la decisió final:

- El codi segueix essent tancat, de manera que mai sabrem realment quin és el funcionament intern ni verificar que el que ens diuen és cert
- Tot i que Apple valora la privacitat, aquest judici de valor es limita a compartir aquesta amb tercers, l'empresa i la seva política de privacitat segueixen tenint naturaleses agressives per tal de recopilar el màxim dels seus usuaris

Com podem veure, la naturalesa d'un codi, obert o tancat, serà determinant en la selecció d'un software determinant, en aquest cas Safari tot i oferir una presentació i una voluntat d'adaptarse a als canvis actuals de com s'enfoca la privacitat, ens fa desconfiar de si realment oferira lo que promet -a part del fet de tenir a Apple al darrere-.

8 Motors de cerca

8.1 La problemàtica de l'historial

Les nostres busqueres es guarden juntament amb la data que s'han produït i algunes informacions addicionals que s'incrementen d'arribar a estar loguejats al navegador, per tant, totes aquestes busqueres estan associades directament amb nosaltres. Aprofundim doncs, ja que qualsevol cosa que busquem es pot associar a l'usuari final, **qualsevol persona pot veure tot el que hem estat buscant**, això adquireix una nova dimensió al problema quan aquesta informació es pot fer publica o donar-se a la llei. Aquí entrem en una petita contradicció dels buscadors "anònims", ja que per política de privacitat molts estan sotmesos a donar aquesta informació d'haver-hi requeriment legal, tot i així'ns, no estan legalment obligats a recaptar aquesta informació dels usuaris: Ho fan per voluntat pròpia. Tot això ens porta a una idea simple però bàsica: Tot i que un buscador pot tenir les millors intencions per a la nostra informació, aquesta pot filtrar-se a tercers.

8.2 Google

Molt similar a com actua el navegador de Chrome, el buscador de Google recull unes dades similars que tracta per millorar l'experiència de l'usuari [27], cosa que es tradueix en una red de busqueres passades i diferents actituds a la web que Google utilitza a favor seu per predir quins resultats s'ajustaran més al perfil virtual que té ell de nosaltres.

Figure 10: Home de Google

La informació recopilada s'adquireix de diferents maneres. Primerament tenim la que el mateix usuari proporciona. Per exemple quan Google ens demana les dades personals (adreça de correu, nom, telèfon...). També es recopila informació a través dels serveis, aquí incloem les dades del dispositiu -és

a dir, la maquina amb la que treballem- i Google la identifica com a nostre. Els registres de servidor emmagatzemen tota la informació cada vegada que fem una petició http. La situació empitjora quan mirem quines dades es registren als servidors, suposem que el nostre dispositiu és un telèfon mòbil, així mateix, en els registres de servidor de google hi figurarien les següents dades:

- Consultes de cerca
- Numero de telèfon
- Numero de telèfon de la persona que ens truca
- Números de desviament, hora i data de les trucades
- Durada de les trucades, SMS i tipus de trucada
- Adreça IP
- Activitat del sistema, idioma i tipus del navegador
- cookies que identifiquen el nostre conte de Google

Com podem veure, la varietat de dades que recull es més gran de la que podríem esperar, per tot lo demès, segueix una filosofia similar a la del buscador Google.

8.3 Bing

Bing és un buscador de Microsoft que té com a orígens els ja conegut Windows Live Search i Live Search. Respecte a la seva política de privacitat, és idèntica a la d'Edge. Bing instal·la cookies en la nostra maquina per catalogar el nostre identificador de busquera, les cookies emmagatzemades tindran a veure amb: Les configuracions, autentificacions i publicitat a mida per cada perfil.

La informació que recull el buscador és molt similar a la que ja recull Google, per tant en aquest aspecte els cercadors van a capturar la mateixa informació.

8.4 Startpage

Startpage és un servei oferit per ixquick, que també es un buscador [28]. La diferencia està en el fet que aquest últim ofereix resultats de múltiples serveis, Startpage serveix només per als resultats que ofereix Google, això si, **sense registrar la adreça IP de l'usuari ni oferir informació a Google** Per altra banda Ixquick retorna els deu resultats més comuns després de comparar amb múltiples buscadors diferents, d'aquesta manera, els resultats de les nostres busqueres son els que han retornat la gran majoria de buscadors.

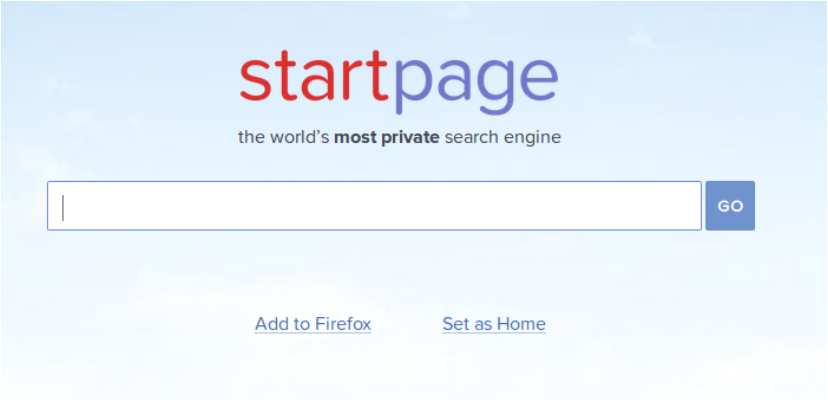


Figure 11: Home de Startpage

La política de privacitat de Startpage comença fent èmfasis en què és la informació personal: "La informació es considerarà personal quan contingui dades d'una persona que serveixen, o poden servir, per a identificar-la" [29]. Aquesta definició té més abast que la de les anteriors polítiques de privacitat ja vistes perquè no només tracta com a personal els noms i la adreça de correu electrònic, sinó també la IP, identificadors i qualsevol tipus de dada que es pugui arribar a relacionar amb la persona física que hi ha darrere l'usuari. Startpage mai registra la adreça IP, només amb l'excepció de quan l'usuari és abusiu, és a dir, fa un gran número de peticions en poc temps, de manera que se'l considera un programa automatitzat. L'única recopilació de dades que fa Startpage és la del número de busqueres que rep cada dia i altres estadístiques no personals.

Només s'utilitzen cookies de preferències i tenen una caducitat de 90 dies, això és una altra distinció respecte als altres buscadors, ja que no emmagatzema cookies d'identificació. Com a detall extra, Startpage també té un generador de URL que elimina la necessitat de cookies -la informació que tenen les cookies s'envia en la mateixa petició de l'URL-. Startpage es blinda en l'àmbit legal marcant dues condicions per tal de compartir la seva informació amb entitats governamentals, primerament només accepta sol·licituds de les autoritats holandeses, que és on tenen la seva seu, i a més a més s'estudia la validesa de la seva sol·licitud i determinen si estan obligats a complir amb el mandat o no.

8.5 DuckDuckGo

DuckDuckGo és molt similar a StartPage en política de privacitat, ja que a grans trets, es pot resumir en què no registren ni comparteixen informació personal.

Ducklingo ataca directament les fugues d'informació que comparteixes amb la petició HTTP [30], això dona una nova dimensió al problema de la privacitat, ja que no només estem compartint informació

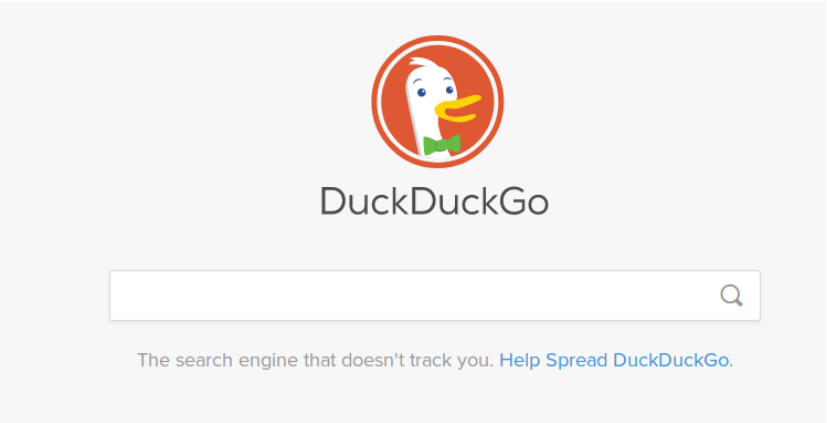


Figure 12: Home de DuckDuckGo

amb el nostre buscador, sinó també amb els llocs on accedim en el nostre buscador. A part, com ja havíem comentat cada vegada que entrem en un lloc web el mateix ordinador envia informació al lloc -IP, sistema operatiu utilitzat, navegador...- Ducklingo en la seva política fa ressò del malestar que pot provocar tanta quantitat d'informació compartida, per això, utilitzant el seu cercador permet no enviar els ítems a altres llocs web. Tot i que els llocs que visitem seguiran sabent que els hem visitat, no podran deduir que hem buscat abans d'arribar a ells ni tenir un històric de busqueres prèvies.

També va un pas més enllà enviant totes les cerques de les pàgines que ho permetin al protocol HTTPS per defecte. D'acord amb la problemàtica de l'historial anteriorment presentada, DuckDuckGo enfoca el problema de la manera més simple: No recollir cap tipus d'informació personal, de manera que queda parcialment solucionada la problemàtica. Tot i així'ns hi ha certa informació que sí que recolleix, similar a searchX, tot i emmagatzemar busqueres, no registren la Ip i només ho fan per tal de millorar el sistema d'autocorrecció ortogràfica, com a últim detall DuckDuckGo té codis d'afiliació amb comerços en línia, de manera que cada busca que acabi conduint a una compra en Amazon o Ebay, de manera anònima, conduirà a una petita comissió per al cercador.

8.6 Yahoo!

Yahoo és un cercador d'informació que ha anat augmentat la seva gamma de serveis (correu, missatgeria, compres ...). La seva política de privacitat segueix una estructura similar a les anteriors però estesa en els punts de quina informació és recopila i comparteixen. Tot i no vendre o llogar aquesta informació recollida, sí que la comparteix amb tercers afiliats o a requeriments legals, afegint també el punt que en el cas de situacions d'il·legalitat o violació dels termes, sera el mateix Yahoo el que compartirà la informació i avisarà d'un ús indegut [36].

Actualment, però, a causa de la fusió entre Yahoo i Oath (companyia de mitjans digitals) [37] que ara formen part de la família d'empreses Verizon la seva política de privacitat ha canviat i ofereix alguns punts important, com ara el fet que els automatismes de Oath podran analitzar els missatges enviats i a partir d'allà (un cop anonimitzada la informació, com ja hem vist en altres serveis) determinar la publicitat més adient per nosaltres. Curiosament, la manera que té Yahoo d'oferir-nos una alternativa és directament eliminar la nostra compta.

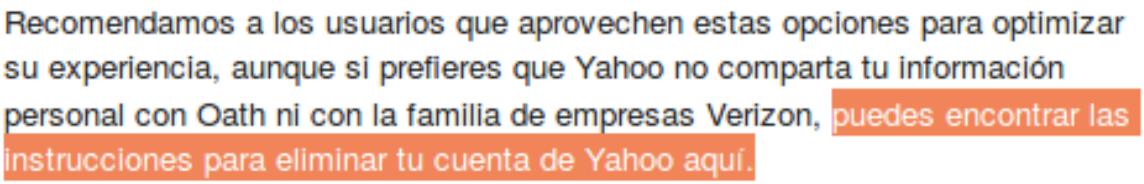


Figure 13: Opcions de privacitat alternatives ofertades per Yahoo!

Yahoo pot ser un exemple clar que és el que no hem de buscar en un cercador que protegeixi la privacitat.

9 Metadades

Abans de parlar de la protecció del contingut dels missatges que enviem, hem de tocar un tema intrínsecament important. Gairebé més important que les nostres dades, les metadades (que li donen context als missatges que enviem) ofereixen el context que les maquines necessiten per tal d'entendre el missatge, context que moltes vegades deixa anar molta més informació de la que hi hauria [38]. Quan parlem de metadada ens podem referir a informació miscel·lània com ara l'autor, data de creació, modificació i mida dels arxius enviats (inclòs el del mateix missatge) [39].

Així mateix, perquè ens haurà de preocupar la metadada des d'un punt de vista estrictament enfocat en la seguretat? Un exemple possible és l'enviament d'una imatge mitjançant un servei de missatgeria, les metadades d'aquest arxiu poden contenir l'hora exacta de creació del fitxer (quan es va fer la foto) i fins i tot les coordenades geogràfiques. Concretament en l'aspecte dels serveis de missatgeria, les metadades amb les quals podem estar tractant poden ser de localització, hardware i connexió entre moltes altres.

9.1 Cas pràctic 1

Per fer una mostra més visual de fins a quin punt es produeix un sangrat d'informació amb les metadades, només hem de veure d'informació completa d'un correu electrònic que hàgem rebut, tot i que la majoria protegiran segons que, la quantitat d'informació revelada és elevada.

Per agafar un exemple, en l'opció de "mostra l'original" en els correus rebuts per gmail, podem veure determinar fins i tot d'ubicació de la persona que ens ho ha enviat. El bloc d'informació que rebem és el següent:

Aquí podem veure per quins nodes ha saltat el missatge des del seu destinatari fins a nosaltres i es demostra un primer punt que havíem intuït: El correu no va directe des del punt A al B. Llegint amb més detall el bloc, podem veure el nom de l'equip que havia enviat el correu i amb un servei de geolocalització de Ip, una aproximació de quina ubicació va néixer el missatge.

Figure 14: Metadades en un missatge de mostra

```
Return-Path: <activitats@afanoc.org>
Received: from PSICOPEDAGOGIA (161.red-80-37-181.staticip.rima-tde.net. [80.37.181.161])
        by smtp.gmail.com with ESMTPSA id u4-v6sm3411299wre.97.2018.04.19.08.32.29
        for <hafidstor@gmail.com>
```

Figure 15: Ip i nom del dispositiu

9.2 Cas practic 2

Suposem que volem extreure tota d'informació d'una imatge que hem rebut per correu, no només el contingut d'aquesta sinó totes les metadades. Només hem de buscar la imatge de la qual vulguem saber més i si estem de sort les metadades d'aquesta ens atorgaran més del que ja teníem. Per exemple, en la imatge següent hem decidit ferla passar per un extractor de metadades en línia.

Un cop passada per al test, el resultat és relativament reconfortant, ja que dades com l'autoria i la localització no han arribat a ser guardades.

En canvi sí que trobem informació del tipus de hardware que ha fet la foto i els detalls del format del tipus d'arxiu, així i tot això torna a demostrar-nos un greu problema de seguretat, ja que el fet que aquesta informació existeixi i estigui tan amagada fa gairebé impossible que ens adonem del seu perill. Per tal d'estalviar-nos mal de caps amb les metadades hi ha múltiples eines per eliminar aquests detalls, el més fàcil d'utilitzar és el sistema de propietats del mateix sistema operatiu, si entrem a les propietats de cada fitxer podem veure els detalls i decidir si esborrar les propietats i d'informació personal.

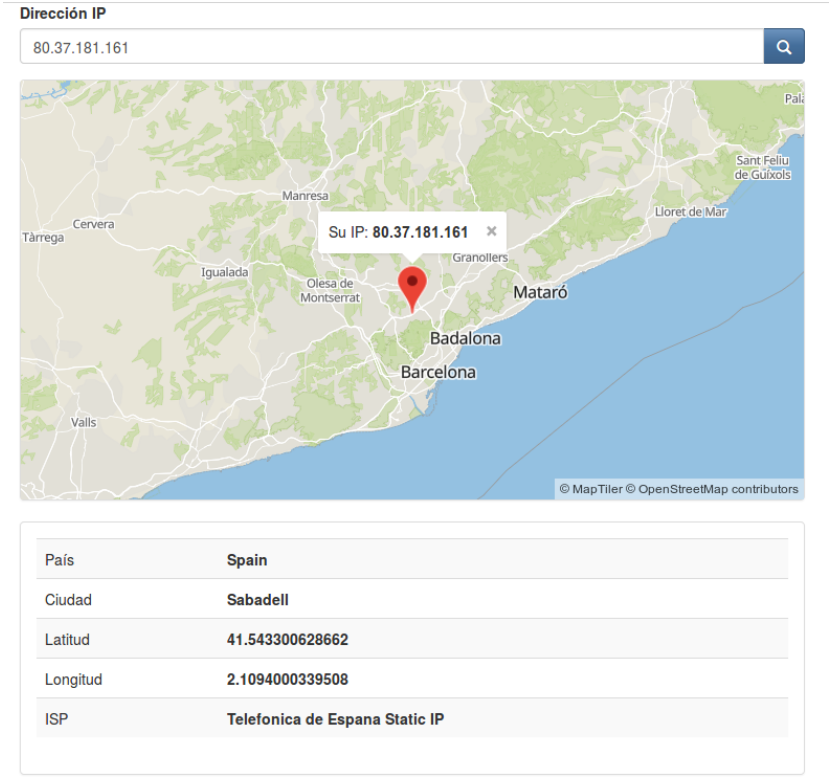


Figure 16: Ip i nom del dispositiu

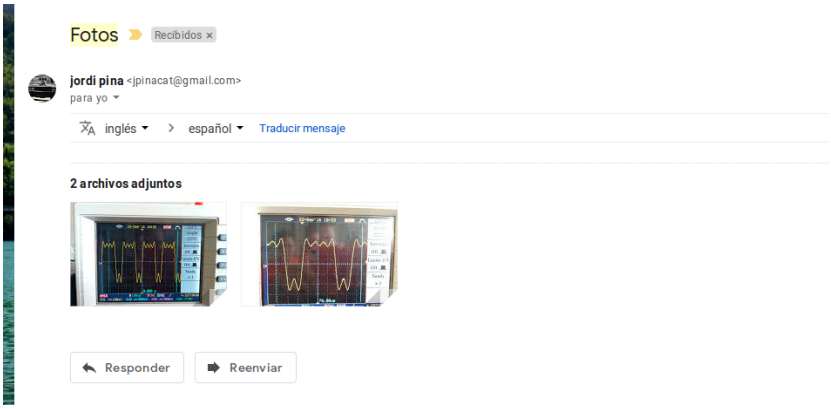


Figure 17: Imatge desitjada

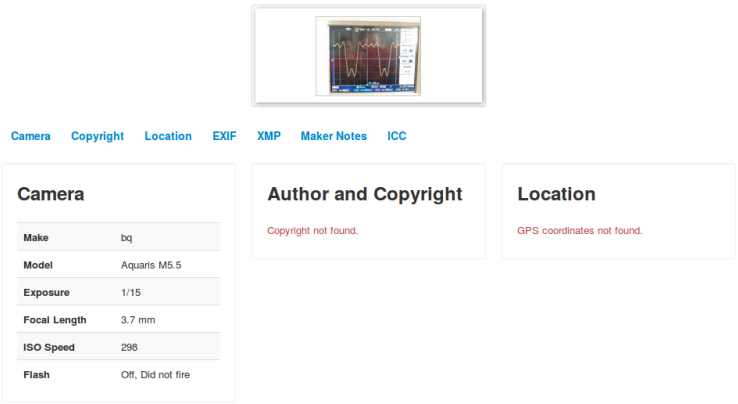


Figure 18: Extracció de metadada I

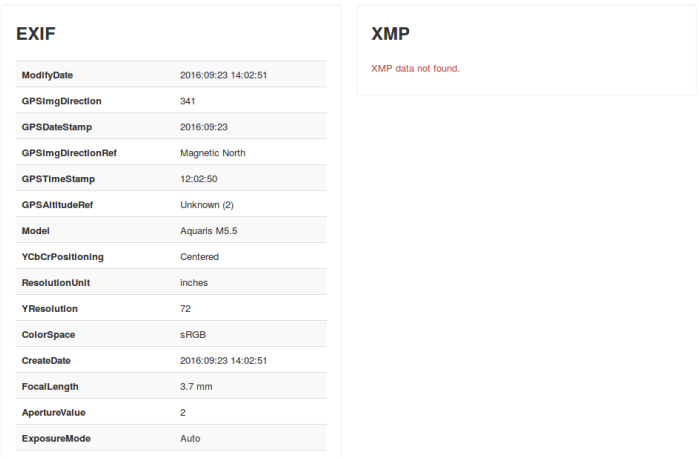


Figure 19: Extracció de metadada II

10 Correu electrònic

El correu electrònic és un dels molts serveis que ofereix la xarxa, tot i que hi ha certa analogia amb el correu postal, les seves similituds acaben allà. Proposem un exemple per a poder-ho exemplificar millor: Suposem que disposem de dos usuaris diferents, A i B, cadascun adscrit a un servidor mail diferent. Així i tot la quantitat de mans per les quals ha de passar el correu abans d'arribar al destinatari pot elevar-se fàcilment a la centena si tenim en compte que pel mig també tenim proveïdors de comunicació i servei.

10.1 Proveïdors

10.1.1 Gmail

Segueix la mateixa política de privacitat ja definida amb els serveis de Google de manera que ens podrem enfocar únicament en les seves funcionalitats com a servei de missatgeria. Hem de considerar que en ser un servei gratuït que ha aixafat la competència gràcies als beneficis que ofereix tals com més giges al núvol o rapidesa en el servei el fan més llaminer. De totes maneres sorgeixen múltiples problemàtiques en tractar-se d'un servei de Google. Primerament tenim el fet del seu monitoratge en forma de còpia dels missatges, tota la nostra correspondència que circuli per Gmail quedarà enregistrada als servidors d'aquest i la seva política ens avisa que pot oferir el contingut dels nostres missatges a qualsevol òrgan administratiu que tingui una ordre judicial. Gmail ofereix moltes característiques positives quan es tracta d'usabilitat per als usuaris, però té suficients taques negres per a no recomanar-lo com a servei de correu Entrarem en més detall amb Gmail en l'apartat de serveis Google.

Figure 20: Logotip Gmail

10.1.2 ProtonMail

ProtonMail és un servei de correu electrònic xifrat que va nàixer arran de les declaracions de Edward Snowden respecte a la vigilància del govern d'estats units. ProtonMail té seguretat per disseny i no per implementació, des del nivell més baix d'aquest ja trobem barreres de seguretat que busquen protegir el seu conte.

Per exemple, cada usuari disposa de dues contrasenyes, una per la conta en si per al login i una altra per a l'accés a la bustia de missatges, un detall important és que la segona contrasenya només la té l'usuari, el servidor no coneix el pass per a la bustia d'accés, de manera que a la banda del servidor

només poden veure les dades de l'usuari encriptades amb una clau que no disposen (al no disposar-la, no la poden donar ni a governs ni a tercers maliciosos).

El xifrat del qual disposa és asimètric de clau publica per tal de tenir-ho xifrat d'extrem a extrem. Encara que el canal de comunicació passi per als servidors de ProtonMail, aquests no tenen possibilitat de recuperar els missatges dels usuaris, ja que estan encriptats amb el parell de claus publica/privada.

10.2 Clients de Correu

10.2.1 Thunderbird

Thunderbird no es estrictament un servei de email, si no un client de codi obert que funciona com a servei de missatgeria, un cop feta la notació, continuem. Darrere d'aquest programa hi ha la fundació Mozilla, cosa que ja ens dona unes certes garanties en els aspectes que ens interessen.

Apart dels beneficis que implica utilitzar un servei de mail que permet no conectar-se a la web per veure la bustia (i per extensió tenir en local una copia de tots els nostres correus), també ens dona funcionalitats com la de poder gestionar múltiples comptes de correu a l'hora o aplicar una capa extra de seguretat en la missatgeria gracies a GPG. Thunderbird está disponible per multiples plataformes, essent recomanable utilitzar-lo amb sincronïa amb sistemes operatius que afavoreixin la privacitat per talt de generar sinergía. Al permetre multiples contes de correu treballar al-hora també ens ofereix treballar amb carpetes comparties entre aquestes.

Figure 21: Logotip ThunderBird

Com podem veure, les caracteristiques ofertades a nivell funcional son variades i s'agraeïxen, de cara a la privacitat, una de les poques coses que ens permet fer que no pugi imitar un servei de correu web és l'eliminació d'alguns headers quan el missatge és enviat, per exemple el header User-Agent, que especifica la versió del nostre sistema operatiu. Per al que fa les demès alternatives de seguretat, ens permet signar missatges amb GPG i aplicar una capa més de seguretat a les nostres comunicacions.

10.2.2 Outlook

Outlook es un client de correu electrònic amb la característiques que esta projectat cap a grups de treball o empreses, permetent una gestió de múltiples usuaris amb les seves busties individuals i compartides. Al ser un software privatiu, totes les promeses son difícils de verificar, aixo sumat al fet que comparteix política amb Microsoft ens obliga a desestimar aquesta opció immediatament.

10.3 Altres alternatives

Suposant que cap de les anteriors alternatives acabi de convèncer a l'usuari final, sempre tenim altres mètodes i serveis per no renunciar al correu electrònic, Mintemail.com i filzmail.com ofereixen la possibilitat de correus d'un sol ús (explicació més detallada del servei)

Tot i així'ns, l'alternativa més clàssica i eficaç seria utilitzar com a servei de missatgeria PGP, és a dir, amb clau publica i privada. El funcionament és simple, cada usuari es genera dues claus, una publica i una privada, utilitzem la clau publica perquè tothom pugui comunicar-se amb nosaltres, aquesta clau la podem penjar on vulguem i enviar-la per qualsevol canal no segur, ja que com el seu nom indica es publica i transferible. La clau privada serveix per desxifrar els missatges encriptats dirigits a nosaltres -aquells missatges que han estat encriptats amb la nostra clau publica-. Alternativament, si volem enviar un missatge només necessitem la clau publica del receptor per encriptar el missatge, missatge que només podrà ser desencriptat per al propietari de la clau privada, això permet enviar missatges completament segurs en canals completament insegurs.

Els serveis anteriors (Com Thunderbird o Gmail) ofereixen possibilitats d'implementar GPG en les seves configuracions, així i tot si volem estalviar-nos software intermediari sempre podem utilitzar directament les eines del sistema operatiu per utilitzar missatgeria GPG.

11 Missatgeria

11.1 Telegram

11.1.1 Que és?

Telegram és una aplicació de missatgeria desenvolupada amb programari lliure. A part de missatgeria estàndard, ofereix transferència d'imatges, vídeos i tot tipus de fitxers a part de la possibilitat de permetre trucades de veu. D'entre les seves funcionalitats, la més brillant consisteix en la seva varietat de possibilitats per facilitar una comunicació segura [42]. Si aprofundim en les seves característiques de seguretat, ens podem trobar que tots els missatges són encriptats, permet xats amb missatges auto destructibles i és de codi lliure, és especialment important recalcar que al ser de codi obert **qualsevol usuari pot veure quin tractament real es fa de la seva informació**.

Telegram és una aplicació multiplataforma, de manera que pot ser utilitzat des de el telèfon mòbil, des de la web o la pròpia aplicació d'escriptori, cap d'elles és millor que l'altre tot i que hi ha algunes característiques (per exemple, el xat secret) exclusives de la versió mòbil. Les aplicacions dintre de Telegram. Des d'un punt de vista estrictament tècnic, l'aplicació de mòbil és recomanable per sobre de les altres si el que busquem és la privacitat. Això no implica que hàgem de deixar d'utilitzar les altres plataformes, només que amb l'app de mòbil les possibilitats de fuga d'informació sensible es redueixen. Hem d'esser conscients també que l'aplicació de mòbil te certes parts privatives -com ara la generació de clau privada o els xats secrets -. Tot i que podem considerar a Telegram com una aplicació de missatgeria segura, sempre hi ha espai per millorar.

Telegram té dues capes d'encriptació, primerament la que separa el client i el servidor s'utilitza en els xats que queden registrats al nuvol (tant privats com grupals), a més a més, els xats secrets tenen una capa extra d'encriptació client-client. L'encriptació que utilitza és de 256 bits i la metodologia d'intercanvi de claus és la de Diffie-Hellman.

Abans d'endinsar-nos en les bones pràctiques per mantenir una comunicació segura, simplifiquem primer els punts més importants de l'aplicació, en aquest cas l'encriptació punt a punt només es dóna en els xats secrets [43], aquests xats no queden registrats en els servidors de Telegram i tenen una vida determinada.

Telegram pot protegir la nostra informació amb eficiència, això implica que tota la informació enviada (text, imatges,fitxers) que s'envii no podrà ser desxifrada pel nostre proveïdor, l'administrador de xarxa o tercers amb intencions malicioses. Així i tot Telegram no pot fer res si algú agafa el nostre telèfon mòbil desbloquejat, l'ordinador de la feina o algun dispositiu que encara tingui la nostra sessió de Telegram oberta (més endavant veurem que **sí que ens podem protegir en alguns d'aquests**

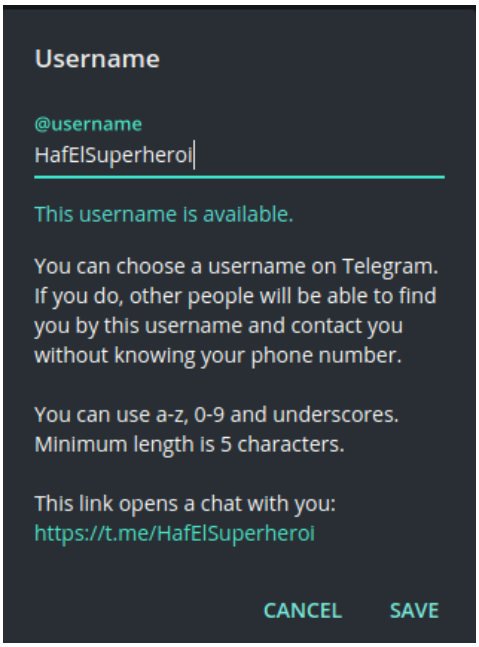
casos

11.1.2 Autoria de missatges

Al fer un re-enviament d'un missatge, estem citant les paraules textuals de l'autor/a, sense que puguem fer cap canvi sobre el qual va dir originalment. En el cas que vulguem fer un re-enviament anònim, és a dir, que no se sàpiga de l'autoria original, haurem de buscar alternatives més recaragolades. Malauradament Telegram no ofereix cap tipus d'eina per fer re-enviaments anònims, d'aquesta manera haurem de buscar alternatives més simples com copiar el text literalment o fer una captura de pantalla obviant el nick de l'autoria.

11.1.3 Nick i Numero de telefon

Per sort Telegram comunica als diferents usuaris mitjançant el seu nick, és a dir, no és necessari que cap dels dos implicats en la comunicació sàpiga el número de telèfon de l'altre.



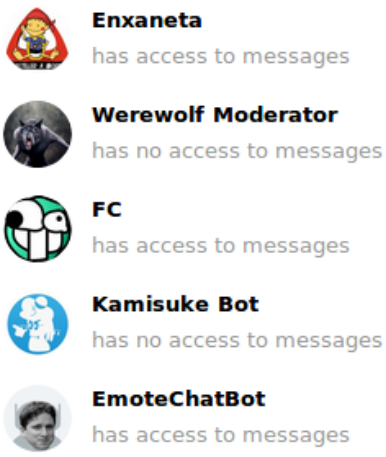
A l'iniciar Telegram, aquest indexa els contactes que tenim registrats al telèfon amb els seus usernames, per sort, d'indexació en el sentit contrari no és possible, podent registrar a altres usuaris amb el username que ens ofereixen però mai arribar a poder saber el seu número de telèfon. Això també s'aplica als xats grupals. Per canviar el nostre Username, només hem d'anar a opcions i seleccionar l'opció Username dintre de l'apartat Info. És recomanable fer-se un nick immediatament després de crear-se una conta de Telegram, ja que aquesta està vinculada directament amb el nostre número de

telèfon, volem mantenir aquest apartat de les nostres comunicacions

11.1.4 Bots de telegram

La plataforma ofereix els bots, que són comptes d'usuaris no associats a números de telèfon i que automatitzen diferents tipus d'activitats [45]. Els usuaris poden interactuar amb els bots enviant-lis missatges o comandes. Els bots poden fer diferents tipus de feina ja sigui notificar notícies, fer jocs o integrar-ho amb diferents serveis com gmail, wikipedia o youtube.

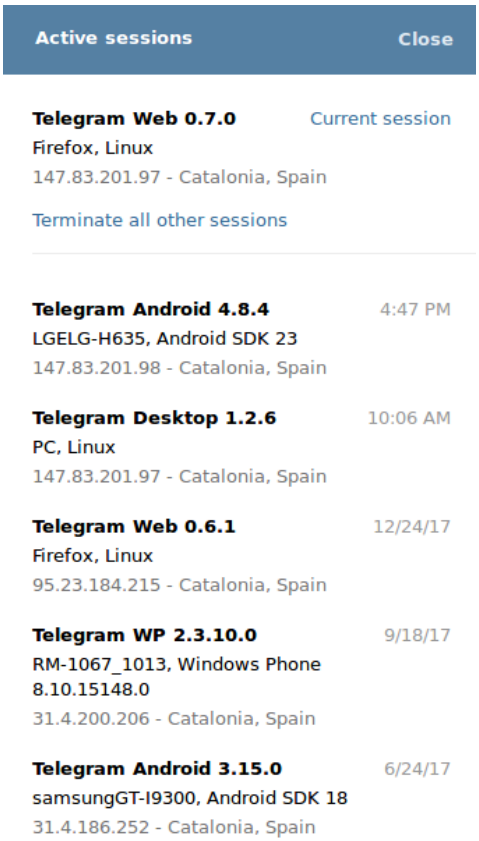
Així mateix els bots poden registrar perfectament tot el que s'escriu en una conversa d'arribar a tenir permís de lectura, ja que molts bots no tenen el seu codi obert a tothom, mai podem arribar a determinar que estan fent darrere les càmeres.



Per tal d'evitar això, li direm als bots que estiguin en mode privacitat, en aquest mode el bot només rebrà missatges que comencin amb una contra barra, missatges de canals o els seus propis. El mode privacitat bé activat per defecte, així i tot, els usuaris poden veure en la llista de membres d'un grup si els bots estan en mode privat o no. Qualsevol bot amb permís de lectura de missatges és un bot perillós, només ens podrem assegurar que aquest no registra la informació d'arribar a tenir accés al seu codi, altrament, haurem de desconfiar d'aquest.

11.1.5 Sessions iniciades

Cada vegada que iniciem sessió en un dispositiu diferent [44], aquesta es queda oberta fins que o bé és esborri l'historial o bé se surti manualment. Per tal de desconnectar-nos definitivament d'un dispositiu, tot i no tenir accés a ell, Telegram té un registre de quins són aquells dispositius on la sessió segueix oberta, de manera que ens permet sortir d'aquests remotament.



Per accedir a les sessions obertes, anirem a opcions i podrem trobar "Sessions Actives". És una bona practica el fer un netejat de sessions de Telegram cada mes aproximadament, la millor manera d'evitar fugues d'informació és limitar els accessos a tercers

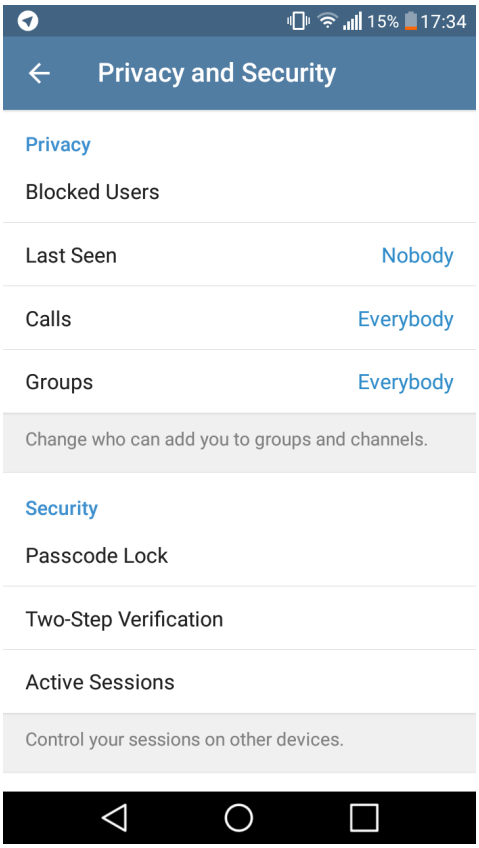
11.1.6 Verificació en dos passos

Un altre afegit en la privacitat i seguretat de Telegram és la verificació en dos passos, això ens permet ficar una contrasenya addicional que ens serà demanada cada vegada que ens loguejem amb la nostra conta a cada nou dispositiu (això en addició al codi que rebem per SMS).

Trobarem la verificació en dos passos en les opcions de privacitat i seguretat, en l'apartat de seguretat. Una capa extra de seguretat mai fa mal, en aquest cas ens estaríem blindant contra qualsevol tercer que volgués iniciar sessió en el seu dispositiu i tingues accés temporal al nostre telèfon mòbil

11.1.7 Borrat de missatges

Com es podria esperar Telegram ofereix la possibilitat d'esborrar missatges enviats a grups o a individuals, amb la complicació que tenim un límit de 48 hores per eliminar-lo completament, el detall està en



què els receptors del missatge el perdran per sempre (aquí ja no entrem en les possibles re-enviaments o captures de pantalla). Per tal de esborrar missatges, només hem de clicar sobre el missatge en concret i ens apareixeran tres opcions: Reenviar, eliminar i respondre. Tot i que a l'eliminar missatges sensibles antics aquests no s'esborrin per a l'altra part receptora, ens estalviem de tenir-los en l'àmbit local, de manera que no afecta tant el límit de 48h.

11.1.8 Bloqueig de dispositiu mòbil

Com ja hem comentat abans, tot i que Telegram no pot evitar que el telèfon caigui a mans de tercers, sí que pot fer certes coses al respecte per tal afegir capes extres de seguretat que dificultaran l'accés a la nostra informació sensible. L'aplicació de mòbil disposa d'un bloqueig d'aplicació, de manera que cada vegada que sortim de l'aplicació i vulguem tornar a entrar ens demanarà una contrasenya de 4 dígits.

D'aquesta manera, si un tercer pogués arribar a accedir al nostre telèfon mòbil hauria de superar una altra barrera de seguretat per poder arribar als missatges guardats de Telegram.

11.1.9 Xats secrets

Tots els missatges del xat secret estan encriptats de punt a punt, això significa que només el receptor i el transmissor poden llegir el contingut d'aquells missatges i cap persona (inclosa Telegram) poden desxifrarlos. A més a més, aquests missatges no es poden re-enviar a altres xats i d'arribar a esborrarlos en una banda de la comunicació, també desapareixeran a l'altra banda.

El xat secret també permet l'activació d'un timer de autodestrucció de missatges. És important entendre que a diferència dels xats normals, tots els missatges d'un xat secret estan guardats específicament al dispositiu que va iniciar el xat i no al nuvol, implicant que des de l'aplicació d'escriptori no podrem veure xats iniciats al mòbil.

Els xats secrets només es poden inicialitzar en l'aplicació de mòbil. Clicarem a la icona de nou xat (te forma de llapis) i en la selecció de contactes, podrem triar si volem un nou grup, nou canal o nou xat secret. La millor manera de no perdre informació personal és directament no tenir-la enlloc. No tot són bones notícies, un petit (gran) inconvenient és que la generació de la clau privada ve donada per part del servidor de Telegram, ja que no podem veure el codi obert de l'aplicació de mòbil ni saber com treballen els servidors, hem de tenir dubtes respecte si el servidor realment emmagatzema la clau de forma segura. Ja que els servidors són tancats tampoc podem saber si realment els missatges dels xats secrets acaben emmagatzemats allà o no. En aquest cas, hem d'actualitzar l'anterior conclusió: **El xat secret és la millor eina de Telegram per la seguretat de punt a punt si i només si confiem en la benevolència del servidor**

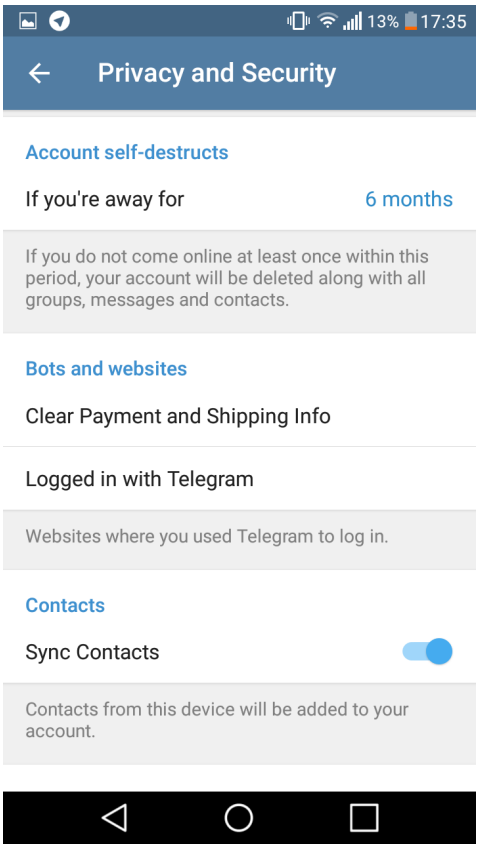
11.1.10 Imatges desades

Tot i que hem ficat una contrasenya d'accés a l'aplicació de mòbil, les imatges que hem descarregat en els diferents xats a segueixen a la memòria del telèfon , així i tot Telegram també ofereix una opció de mantenir les fotografies en el nuvol, aconseguint així que d'informació sensible no quedi registrada al nostre dispositiu

El desbloqueig d'imatges desades a la galeria el trobarem a opcions; Missatges, allà podrem desactivar l'opció de desat. Tenir redundància d'informació pot ser perjudicial, ja que tenim les còpies de les imatges enviades i rebudes al nuvol, no és necessari tenir-les a la memòria interna del telèfon. Per tant es pot considerar com a bona pràctica desactivar aquesta opció i no omplir el dispositiu d'imatges redundants.

11.1.11 Autodestrucció

Un altre dels aspectes més importants dels xats secrets és la possibilitat d'activar l'opció d'autodestrucció dels missatges en aquells xats, això fa que tot el que enviem tingui una data de caducitat que podem determinar nosaltres mateixos, variant entre 1 segon i 1 setmana.



A part, també disposem de la possibilitat d'autodestruir la nostra conta completament d'arribar a estar durant un llarg període sense interactuar amb l'aplicació. Com sempre, la millor manera de no perdre informació és directament no tenir-la, per això l'autodestrucció de missatges hauria d'anar sempre acompanyada del xat secret. L'autodestrucció de comte d'usuari pot ser una bona manera d'eliminar completament el nostre usuari donat el cas que no tinguem més accés a ell.

11.2 Whatsapp

El servei de missatgeria actual més conegut és el Whatsapp, fem una rapida mirada a la seva política de privacitat per posar-nos en escena. Un dels primers punts i el que pot cantar més d'introducció és que Whatsapp fa uns anys va passar ser part del grup d'empreses de Facebook, tot i que asseguren que la comunicació d'informació sensible es compartirà amb Facebook, però això no es pot demostrar.

No és estrany trobar-se notícies de forats en la seguretat de Whatsapp, tot i així'ns una encriptació dels missatges d'extrem a extrem ens dóna una certa seguretat per al que respecta la privacitat en les comunicacions.

Informació de l'usuari	
Temps de generació de l'informe	2018/09/16-14:30:04
Data de sol·licitud de l'informe	2018/09/13-11:30:52
Número de telèfon	+34617267342
Nom	–
Estat de la connexió	OFFLINE
En línia desde	–
Desconnectat desde	2018/09/16-13:42:15
Inactiu desde	–
Última IP de connexió	31.4.203.0
IP de connexió actual	–
Tipus de dispositiu	Android
Versió de l'aplicació	2.18.277
Número de sèrie del dispositiu OS	7.1.1
Fabricant del dispositiu	Sony
Model del dispositiu	F5121

Figure 22: Parametres enregistrats de Whatsapp

Així mateix, també se li pot demanar a Whatsapp una còpia de les dades que té de l'usuari. Entre aquestes dades, podem trobar quins són els números dels nostres contactes, els horaris D'última connexió i els grups en els quals estem ficats.

11.3 Signal

En la seva política Signal insta a què la privacitat està aplicada des de la capa de disseny, de manera que és un aspecte present a tots els nivells de l'aplicació [46]. Signal és un sistema de missatgeria mòbil que està dissenyat des de la base per enfocar problemes de privacitat i seguretat. Com a altres sistemes de missatgeria, Signal ofereix la capacitat d'encriptar tots els missatges enviat, a més a més, els servidors tampoc registren cap tipus de dades, de manera que cap agència internacional o govern pot demanar-les. Molt similar a Telegram, el seu codi és obert. A part de tenir una encriptació end-to-end, aconseguint que l'accés dels missatges enviats únicament els tingui el recipient amb accés físic al telèfon, també tenim la possibilitat d'encriptar tots els missatges del telèfon, limitant completament

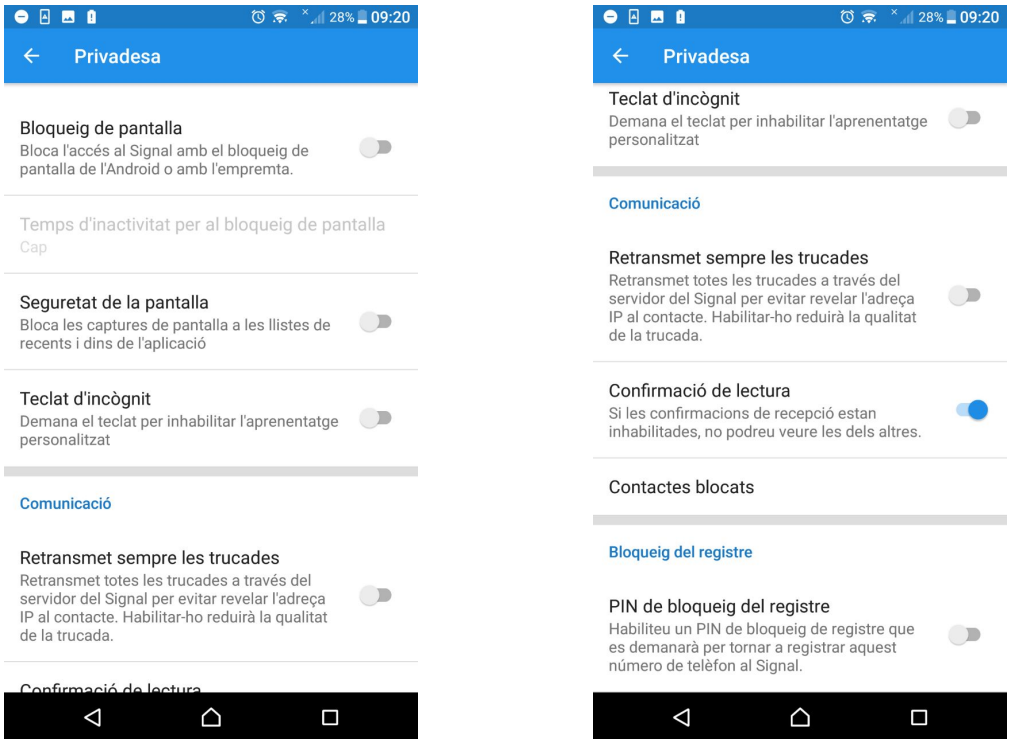


Figure 23: Opcions de privacitat a Signal

les possibilitats de fuga d'informació.

Si fem una repassada a les opcions de privacitat de l'aplicació, ens sorprendrà veure la varietat d'aquestes. Podem trobar inicialment el bloqueig de pantalla, aquest bloqueig de dispositiu similar al de Telegram ens serveix per a protegir qualsevol intent d'accés físic al telèfon.

Una funcionalitat important és la del bloqueig de registre, aquest és un número que Signal ens demanarà a intervals de temps irregulars, serveix principalment per evitar que qualsevol altre usuari intenti registrar-se amb el mateix número de telèfon, això també pot evitar una casuística donada en Whatsapp, donada una línia de telèfon que quedes abandonada (fos degut a no pagar o altres), si un nou telèfon és registres a l'aplicació, hi hauria un conflicte d'identitats, resultant en el segon telèfon aconseguint tots els contactes del primer. Una opció que no ens apareix però que està activa és la d'entrar d'incògnit en un grup. Un cop invitat en el grup en qüestió, podem decidir que ni la fotografia ni el nom d'usuari siguin visibles per als altres participants.

11.4 Comparativa entre sistemes de missatgeria

En aplicacions mòbils un dels determinants en el grau real de privacitat oferit és la quantitat (i quins) permisos demana, tot i que els opcionals poden variar, els que són realment importants són

els obligatoris, ja que són requerits per tal que l'aplicació funcioni. Tant Telegram com Whatsapp demanen obligatòriament els contactes a diferència de Signal, que permet començar conversacions escrivim el número de contacte sense registrar-lo [47]. Els mòbils ofereixen una dinàmica diferent en la protecció de dades comparats amb els ordinadors, ja que aquests poden ser requisats o algú pot tenir accés físic als nostres dispositius sense que en siguem conscients això implica que ha d'existir una capa extra de seguretat de cara a l'aplicació. Tant Telegram com Signal permeten una protecció d'accés a l'aplicació mitjançant un codi d'accés [48]

Qualitats	Whatsapp	Telegram	Signal
Permisos	Contactes obligatoris	Contactes obligatoris	Contactes Opcionals
Protecció d'applicatiu	-	Disponible	Disponible
Metadades	Variades*	Totes aquelles relacionades amb l'aplicatiu al nuvol	Mínimes (hora de connexió i numero)
Xifrat	Extrem a extrem	Extrem a extrem**	Extrem a extrem
*Ip, nom de red, número de telefón			
**Només en xat secret, no per defecte			

Figure 24: Comparativa serveis de missatgeria mòbil

Tal com ja hem comentat al punt de metadades, el contingut d'aquestes és gairebé tan important com el del mateix missatge, oferint context al seu contingut. Whatsapp recopila metadades com Ips, nom de la xarxa, número de telèfon entre moltes altres, mentrestant Telegram en ser un servei basat en el núvol ho té tot allà (fotos, arxius i conversacions no xifrades) [41]. Signal manté al mínim les metadades fins al punt que només emmagatzema la data de última connexió i el número de telèfon del nostre conte.

De cara al xifrat, el més important (d'extrem a extrem) només està habilitat per Whatsapp i Signal, mentre que Telegram s'activa mitjançant el xat secret. Com que el cas ideal és que el xifrat estigui present en tot moment (sense servidors intermediaris), les opcions que ja ens venen per defecte són preferibles.

Respecte per al que fa sistemes de correu, tot i que tenim alternatives al gegant gmail com ara utilitzar altres serveis com Protonmail o correus d'un sol ús, hem de ser conscients que per molt que ens protegim nosaltres com a remitent, si aquest missatge acaba sent enviat a una bustia de gmail o outlook tot els nostres esforços quedarien en va, per això el clàssic i confiable GPG/PGP és l'alternativa més segura i solida, com a únic inconvenient a aquest mètode tenim la dificultat que pot comportar aquesta eina per a un usuari novell. A causa de aquesta barrera que pot suposar el fet de perdre tanta usabilitat, podem trobar múltiples connectors que emulen les funcionalitats de PGP i les apliquen al

servei que decidim (ja sigui Gmail, outlook o thunderbird) [40].

12 Case Study: Registres Google

Google i tot el conglomerat de serveis que ofereix ens dóna l'opció de descarregar un fitxer que segons ells és tota la informació que tenen enregistrada de nosaltres [49], tot i que no ens podem fiar de què això sigui cert i no hi hagui més cosa amagada, ja és un principi poder veure quin conjunt de dades *mostrables a l'usuari* està enregistrant, així doncs, anem a fer un anàlisi exhaustiu del fitxer que ens ofereix Google, o vist des d'una altra manera, quina de les moltes petjades inesborrables ha deixat el nostre perfil a la xarxa [50].

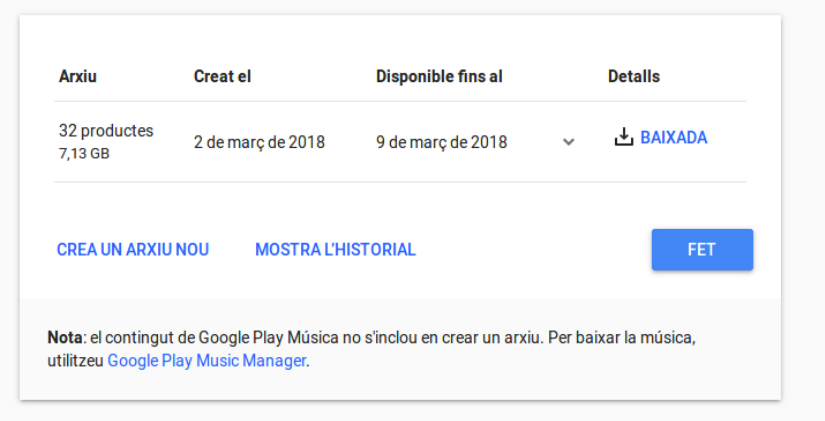


Figure 25: Takeout de informació

Un cop tenim disponible el fitxer, la primera curiositat que trobem és el seu pes, aproximadament 7gb's d'informació han sigut enregistrats d'ençà que es va crear la conta fins al moment, tot i que aquesta dada pot canviar significativament depenent de l'ús que en faci cada usuari, ja ens dóna una idea aproximada de quin volum de dades estem parlant. L'enregistrament es dóna a diferents nivells, cadascun d'ells relacionat amb un servei diferent.

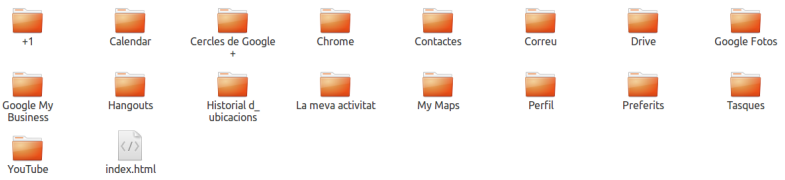


Figure 26: Carpetes del takeout

12.1 Chrome

Per al que fa el navegador de Google, aquest emmagatzema, entre altres, quines són les nostres adreces preferides i les extensions que hem afegit entre altres. Primerament el JSON d'autoemplenament de dades (estructura de dades nativa de javascript) podem trobar qualsevol instància afegida a les opcions d'autoemplenat de Chrome com la següent:


```
        {
            "name_first": ["Hafid"],
            "address_home_country": "ES",
            "address_home_sorting_code": "",
            "address_home_state": "BARCELONA",
            "address_home_dependent_locality": "",
            "address_home_city": "manresa",
            "address_home_language_code": "",
            "name_full": ["Hafid Kharbouch"],
            "origin": "https://www.amazon.com/gp/buy/addressselect/handlers/
display.html",
            "name_last": ["Kharbouch"],
            "name_middle": [""],
            "use_count": 5,
            "email_address": [""],
            "company_name": "",
            "address_home_line1": "carrer de circumval·lació 106-1a",
            "address_home_line2": "carrer de circumval·lació 106-1a",
            "guid": "26217B12-337C-45AD-A61F-A2A47CBFA6BF",
            "address_home_zip": "08241",
            "address_home_street_address": "carrer de circumval·lació 106-1a\ncarrer
de circumval·lació 106-1a",
            "phone_home_whole_number": ["637 00 76 73"],
            "use_date": 1486160029
}
    ]
```


Figure 27: JSON amb els parametres d'autoemplenat

També tenim el fitxer d'adreces d'interès, que té totes les dades d'interès afegides per l'usuari (inclòs les que van ser esborrades en el seu moment). El fitxer d'extensions també té un historial detallat de quan es van instal·lar i quins paràmetres tenien actius en el moment de la presa de dades.

Amb aquesta petita mostra podem veure un dels perills d'utilitzar Google Chrome sincronitzat a una conta Google, l'extensió de fins a quin punt ha quedat enregistrat tot és important, tot i que la part més preocupant no deixa de ser que tot això ha sigut voluntari, l'usuari és qui té la decisió final d'utilitzar aquests serveis i desencadenar en aquest resultat.

12.2 Contactes

Android ofereix la possibilitat de sincronitzar la nostra llista de contactes amb la de Google per tal de facilitar el traspàs d'aquests en cas que canviem de telèfon mòbil, tot i que aquesta utilitat pot semblar positiva en un primer instant, també és perillosa com que aquests contactes han de quedar emmagatzemats en el nuvol per la seva posterior recuperació, en el takeout de dades personals oferit per Google, hem trobat aquest fitxer. Per sort gràcies a un acte de prevenció, en la conta que estem analitzen en cap mai s'han emmagatzemat contactes relacionant-los amb el correu electrònic de gmail,

deixant-nos amb un fitxer buit.

Així i tot, el fitxer de contactes de correu és inevitable que no enregistri informació, en aquest podem trobar un llistat detallat de correus amb els quals hem tingut contacte i de ser possible, el seu nom complet. En el cas dels correus, podem defensar que Google té més catxe per justificar l'emmagatzemament d'aquests, ja que per enviar futurs correus a contes ja conegudes no guardar-los seria una pèrdua innecessària.

12.3 Correu

Un dels serveis més coneguts per Google és el servei de Gmail que ja hem analitzat prèviament, és intuïble que el takeout d'informació tingui un contingut extens, i de nou, serveis Google no decepciona. Ens trobem amb un fitxer de text de 2,1 Gigabytes que conté absolutament tots els correus enviats, rebuts i de correu brossa. Com hem dit abans, també queden enregistrats els contactes de correu amb els que he intercanviat missatges:

```
FN:Eudald Camprubí
N:Camprubí;Eudald;;;
EMAIL;TYPE=INTERNET:e.camprubi@iskra.cat
END:VCARD
BEGIN:VCARD
VERSION:3.0
FN:F. Xavier Moncunill
N:Moncunill;F.;Xavier;;
EMAIL;TYPE=INTERNET:xavier.moncunill@upc.edu
END:VCARD
BEGIN:VCARD
VERSION:3.0
FN:Francesc
N:;Francesc;;;
EMAIL;TYPE=INTERNET:francescm@epsem.upc.edu
END:VCARD
BEGIN:VCARD
VERSION:3.0
FN:Francisco del Águila
N:del Águila;Francisco;;;
EMAIL;TYPE=INTERNET:fd.aguila.l@gmail.com
END:VCARD
BEGIN:VCARD
VERSION:3.0
```

Figure 28: Contactes enregistrats a gmail

Dintre de Correu també farem incís en el servei de hangouts que és el servei de xat de Gmail, podem trobar el json de conversacions que hem tingut al llarg del temps:

```
"chat_message" : {
  "message_content" : {
    "segment" : [ {
      "type" : "TEXT",
      "text" : "beneficis de fer la practica entre 3424324 persones",
      "formatting" : {
        "bold" : false,
        "italics" : false,
        "strikethrough" : false,
        "underline" : false
      }
    } ]
  }
},
"event_id" : "84UiMBsqVLk87hgGz6Agwa",
"advances_sort_timestamp" : true,
"event_otr" : "ON_THE_RECORD",
"delivery_medium" : {
  "medium_type" : "BABEL_MEDIUM"
},
"event_type" : "REGULAR_CHAT_MESSAGE",
"event_version" : "1450207881103372"
```


Figure 29: JSON que enregistra les conversacions

12.4 Drive

El famós servei d'emmagatzematge gratuït de Google tampoc s'escapa d'aquest enregistrament massiu d'informació personal, en aquest cas, el takeout ens ofereix una còpia total de tots els fitxers enregistrats al servei de Drive en el moment que vàrem demanar la còpia de registres, saber si aquests fitxers un cop eliminats queden esborrats per sempre o si simplement canvien carpeta és un salt de fe.

12.5 Ubicacions

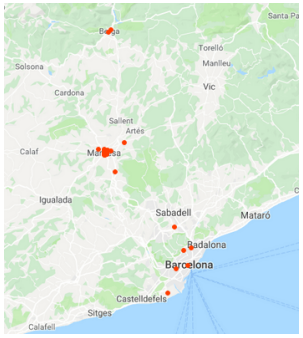
El servei d'ubicacions de Google ofereix un resum mensual dels diferents llocs als quals hem estat si hem anat movent-nos amb un telèfon que te activada d'ubicació -a més que haguem acceptar els obtusos termes d'ús -. Aquest resum efectivament també queda enregistrat als seus servidors, oferint un historial d'ubicacions amb latituds detallades.

Curiosament, també veiem quines són les estadístiques del mitjà de transport que estàvem utilitzant en aquell instant. Això implica que si tenim els serveis d'ubicació activats, aquests enregistren on i quan estem en tot moment. Aquí també hi ha detalls de cap a on anàvem en determinada hora i quin transport estàvem utilitzant per arribar a cert lloc.

En els diferents serveis que podem trobar de Google, tenim entre altres la nostra activitat recent, o el que ve a ser que hem estat fent a tots nivells, per exemple les nostres cerques, les aplicacions utilitzades amb Android, les cerques a la store d'aplicacions i cerques en YouTube.

12.6 Google Analytics

Analytics és un servei de Google que ofereix estadístiques a les pàgines webs que el requereixin, aquest servei ofereix diferents informes com ara quines seccions de la pàgina web són més visitades, la quantitat de resultats d'aquestes pàgines en indexació dels buscadors d'entre molts altres. En l'àmbit tecnològic,




```
"timestampMs" : "1511507601088",
"latitudeE7" : 417370729,
"longitudeE7" : 18287719,
"accuracy" : 17,
"altitude" : 317,
"activity" : [ {
  "timestampMs" : "1511507606025",
  "activity" : [ {
    "type" : "STILL",
    "confidence" : 75
  }, {
    "type" : "IN_VEHICLE",
    "confidence" : 10
  }, {
    "type" : "IN_ROAD_VEHICLE",
    "confidence" : 10
  }, {
    "type" : "ON_BICYCLE",
    "confidence" : 7
  }, {
    "type" : "UNKNOWN",
    "confidence" : 3
  }, {
    "type" : "IN_RAIL_VEHICLE",
    "confidence" : 3
  }, {
    "type" : "ON_FOOT",
    "confidence" : 2
  }, {
    "type" : "WALKING",
    "confidence" : 2
  } ]
}, {
```


Figure 30: Servei de geolocalització de Google

per utilitzar analytics s'han d'afegir línies de codi JavaScript en les pàgines que es volen analitzar, a partir d'aquí el monitoratge és constant en aquella pàgina i l'administrador adquireix resultats de les estadístiques que ell vol [52].

Tot i que la política de privacitat d'Analytics avisa als seus usuaris que no poden recollir informació que permeti identificar a un usuari, de manera que un formulari de registre no només quedaria enregistrat a la base de dades del servei en qüestió, sinó que també depenent de la situació podria acabar a l'usuari d'Analytics que hagués enregistrat aquestes dades.[53]

Ens trobem amb un servei que de per si és benèvol i ja insta en la seva política des de bon principi a no enregistra informació que pugui permetre identificacions, així i tot mal utilitzat pot provocar situacions on informació sensible pot quedar duplicada, tant per al servei com per Google, duplicant també el perill que aquesta informació caigui en males mans.

12.7 Conclusió

Tot queda enregistrat, d'una manera o altra hem analitzat com un dels gegants de la xarxa té un monitoratge gairebé total sobre nosaltres, el previ estudi ha servit per veure l'extensió de fins a quin punt la nostra empremta digital supera el mida que creiem:

També podem accedir a aquesta informació en format web en els detalls del nostre usuari Google, allà podem veure un resum diari de tota la nostra activitat, inclòs quan i on.

Recordem que **tota** aquesta informació pot ser oferida a qualsevol govern amb l'ordre judicial corresponent, sense que nosaltres ho sapiguem i el que és més, sense poder fer res per evitar-ho. Tenim l'alternativa d'esborrar d'informació enregistrada segons Google, però això provoca té dos inconvenients:

Figure 31: Tracking de dispositius utilitzats

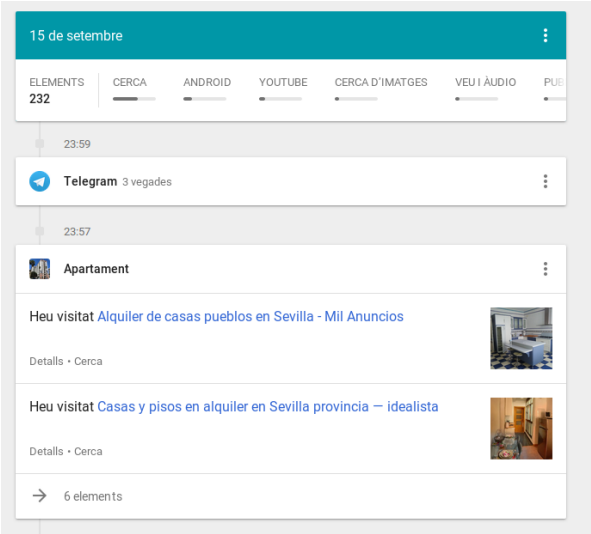


Figure 32: Tracking de activitat detallat

- Aquestes dades es queden durant un cert temps al seu servidor per tal de estar disponibles per a requeriments legals
- No tenim una certesa total de que aquestes dades simplement no canvien de carpeta

D'altra banda plantejar que Google manté d'informació esborrada per sempre no és eficient des d'un punt de vista econòmic, ja que el cost d'emmagatzematge creixeria exponencialment al llarg dels anys. Així doncs, ens trobem en una situació on totes les nostres dades estan essent enregistrades sense pausa i qualsevol moviment que fem queda guardat en una base de dades a la que mai accedirem, amb la possibilitat d'esborrar-les i confiar en què es queden esborrades [51]. D'aquesta manera, ja haguen fet l'anàlisi dels serveis que ofereix Google, podem arribar a una de les conclusions més clares del projecte: **Evitar en la seva totalitat els serveis que ofereix Google**.

Paral·lelament, també podem decidir que els serveis són benèvols i que en cap moment les nostres dades són utilitzades per altres coses no estipulades en la política de privacitat, aquesta decisió es

basa completament i exclusivament en la confiança, si fem l'exercici de veure les nostres opcions, l'alternativa a no utilitzar els serveis, és dipositar tota la nostra confiança en la bondat del servei, per defecte, també podem acceptar el fet que la fuga d'informació és inevitable. Sigui com sigui, ens trobem en una situació en l'última paraula la té el servidor, sigui com sigui, les possibilitats que la nostra informació estigui compromesa són elevades.

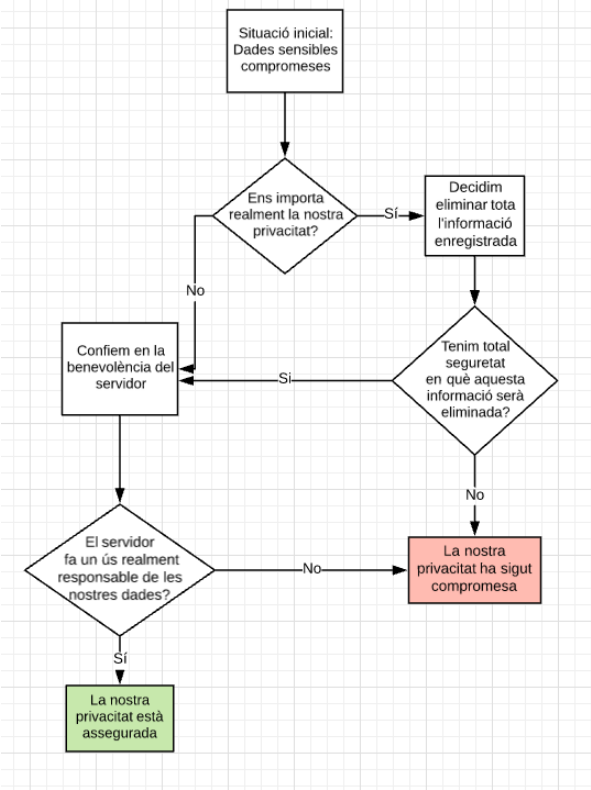


Figure 33: Diagrama de la qüestió de confiança

13 Perfilat social

Entenem per a perfilat social totes aquelles eines que utilitzen les xarxes per determinar una publicitat dirigida a un perfil determinat a partir de diferents paràmetres entre els quals podem trobar edat, sexe, educació.

Per fer-nos una idea de fins a quin punt arriba aquest tracking constant, utilitzarem l'aplicació de Lightbeam[54], una extensió de Firefox que ens permet veure quantes pàgines realment estan monitoritzant els nostres moviments quan naveguem, per fer la prova, simularem un comportament d'un usuari normal en qüestió de pocs minuts:

Inicialment, obrirem el correu i mirarem quines són les últimes notícies en el nostre diari d'elecció, en aquest cas CNN, finalment farem una repassada a quins missatges ens han arribat a Telegram.

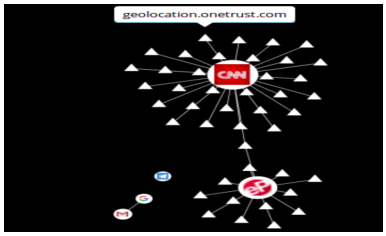


Figure 34: Tracking de webs alienes a les visitades, part 1

Com podem veure en el graf, les figures rodones són les webs visitades mentre que els triangles són trackers relacionats amb aquestes, la majoria són subdominis de la mateixa web, Però també trobem alguns de Facebook, dominis de geolocalització i apis de Google. Si decidim entrar a una xarxa social i buscar algun producte d'Amazon, la densitat del graf creix encara més, curiosament, al provar amb altres serveis de notícies podem veure com hi ha webs de tracking que estan interrelacionades.

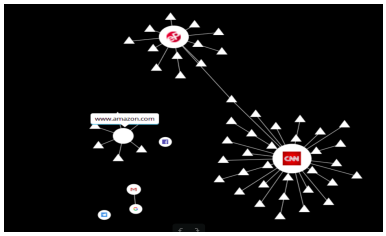


Figure 35: Tracking de webs alienes a les visitades, part 2

Si fem l'experiment de navegar la xarxa durant 10 minuts mentre anem saltant entre diferents webs que ens interessen, podem acabar tenint un graf similar a aquest:

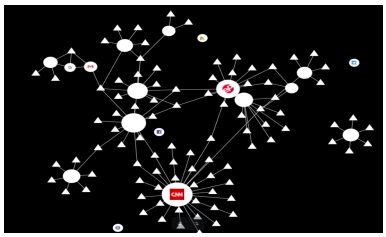


Figure 36: Tracking de webs alienes a les visitades, part 3

Recalcar que les pàgines que actualment hem visitat són les formes circulars, tots els triangles són tercers que observen cadascun dels nostres passos, cada clic que fem queda enregistrat per aquests. El graf ens dóna un resum de la proporció resultant:

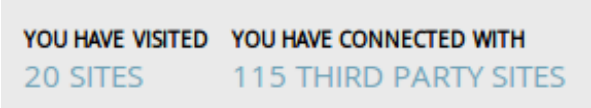


Figure 37: Proporció total de webs visitades/Trackes

Tot aquest monitoratge constant queda elevat quan entrem en el món de les xarxes socials. Tot i que podem considerar que un perfil social pot ser positiu per a certes activitats (un estudiant buscant feina, per exemple), també hi ha l'altra cara de la moneda, l'emprenta que deixem (tant publica com privada) és gairebé impossible d'esborrar un cop publicada a la xarxa.

14 Xarxes Socials

Un concepte de per si que ja és perillós, en una xarxa on el principal material i contingut penjat és informació personal, estan dissenyades de tal manera que per funcionar necessiten que una informació prèviament privada passi a ser de domini públic, així doncs, la fuga d'aquesta es pot donar per feta. Així i tot, avui en dia la discussió no està en quina informació penjem en aquestes xarxes, si no fins a quin punt els administradors d'aquesta poden interactuar totalment amb ella[55].

Sistemes de xarxes socials com aquest xoquen amb qualsevol pretensió de privacitat, ja que els beneficis que en treuen aquestes empreses és precisament el màrqueting específic que generen gràcies a la informació personalitzada de cada individu. A més a més, el significat de la protecció d'informació sensible canvia, si abans el que buscàvem era protegir-nos del proveïdor del servei, el que en moltes xarxes socials es protegeix és el que els altres usuaris veuen de nosaltres, deixant al servei a una capa superior que per lògica no tenim control sobre ella, l'administrador de la xarxa social necessita saber-ho tot de l'usuari perquè aquesta pugui seguir funcionant. A més a més, ens trobem amb un altre factor que multiplica els riscos de fuga d'informació: Les amistats. El principal producte de les xarxes socials és la connexió entre múltiples perfils d'usuaris, de manera que encara que vulguem protegir la nostra conta de cara a altres usuaris, la possibilitat que siguin les nostres pròpies amistats les que ofereixin aquesta informació sense volguer i que aquesta quedi enllaçada al nostre perfil són extremadament altes.

Llavore'ns sorgeix la pregunta de si realment és compatible l'ús d'aquests aplicatius i el principi de privacitat, i de ser així, quins són els casos que fan un ultratge menor de les dades sensibles dipositades, estudiarem quina és l'aplicació que suposa el mal menor. Centrarem l'estudi en les xarxes més utilitzades del moment, tals com Twitter, Instagram i Facebook.

14.1 Twitter

D'acord amb la seva política[56], tots els nostres missatges poden ser llegits per qualsevol altra persona, oferint-nos així i tot la possibilitat de fer-los privats o operar la nostra conta des d'un pseudònim. Respecte a les dades que enregistra de nosaltres, les obligatòries són el tipus de dispositiu des de el que estem connectats i la IP d'aquest, totes les altres dades (correu, número de telèfon, llista de contactes) són opcionals i s'utilitzen per determinar possibles gustos. Tenim diferents opcions per configurar quina informació es publica i quina no.

De nou veiem que tot està enfocat de cara a l'experiència amb altres usuaris i són poques les opcions que ofereix per tal que ell com a servei redueixi la recol·lecció de dades. Similar a Telegram, en cara que tinguem un xat privat (en aquest cas, tweets privats), l'aplicació no ofereix protecció alguna de

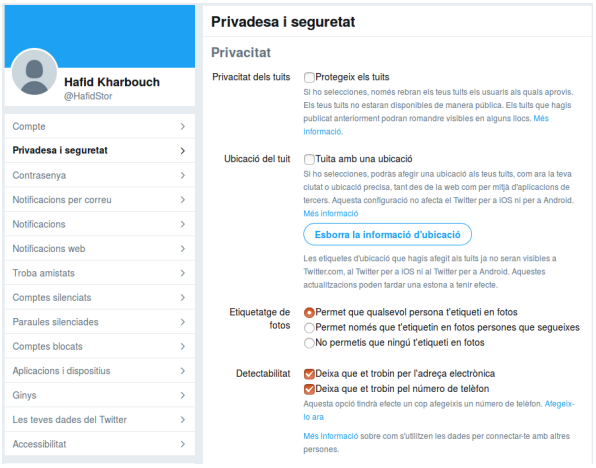


Figure 38: Opcions de privacitat de Twitter

cara al fet que qualsevol seguidor difongui aquesta informació, tornant al punt que havíem introduït en el que en les xarxes socials el sangrat d'informació és més complicat d'evitar per culpa de la seva naturalesa intrínseca. Tot i així'ns, podem considerar que , dintre del que cap, Twitter no és tan invasiu com els seus alterns [58].

14.2 Facebook

La xarxa social més utilitzada del planeta, i per extensió, la fuga més gran de privacitat voluntària que podem trobar. Facebook des d'un primer moment ens demana dades personals com la ubicació, el lloc de naixement i fins i tot ens insta a registrar-nos amb el nostre nom real. Tot i que inicialment l'excusa de la necessitat d'informació personal pot valdre amb el pretext que és per oferir una millor experiència d'usuari, aquest argument cau per si sol quan d'entre tota aquesta informació se n'extreu la metadada i la xarxa comença a enregistrar dades com on vam fer tal foto o des de quin dispositiu vàrem accedir en determinat instant, molt similar a la vigilància dels serveis Google [57]. D'entre altres coses Facebook, igual que Google, també ens permet demanar un takeout per veure quines són les dades que ha anat enregistrant de nosaltres al llarg del temps.

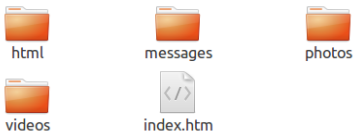


Figure 39: Takeout facebook

Aquí podem trobar totes les conversacions que hàgem tingut, estats que ens hagin agradat i totes les fotos penjades, tot i que arribats a aquest punt, ja no ens sorprèn aquest registre constant d'informació. Abans d'anar al següent apartat, hem de deixar clar que en cap moment Facebook ven la nostra informació a tercers, simplement ven L'accés al nostre mur de notícies per a ficar anuncis determinats d'acord amb el perfil digital que tingui de nosaltres [**?**]. Pot semblar una petita diferencia, però en l'àmbit judicial ha sigut suficient per permetre la seva supervivència.

14.3 Instagram

Instagram és una xarxa social que s'alimenta principalment de les fotos que els usuaris li ofereixen, molt similar a Facebook Però centrada únicament en un tipus de contingut multimèdia, a voltants de 2012, l'empresa va ser absorbida per al conglomerat Facebook, així doncs, les mateixes aplicacions de Facebook i Instagram poden transaccionar informació entre elles si tenim una conta enllaçada en els dos serveis, multiplicant al quadrat. Tot el que hem dit anteriorment respecte a la xarxa de Facebook també s'aplica aquí.

Similar a algunes característiques de Facebook, Instagram va un pas més enllà a l'utilitzar tecnologia de reconeixement facial per determinar la nostra presencia en fotos alienes [59]. En determinats punts de la seva política trobem que cerca informació compartida amb altres usuaris seguirà existint tot i després d'esborrar la nostra conta com que Instagram no la considera nostra.

15 Polítiques de privacitat

Fins ara hem estat mencionant les diferents polítiques de privacitat visitades per anar veient fins a quin punt els productes que oferien eren segurs, en alguns casos hem pogut veure gairebé immediatament si es tractaven de serveis que podrien protegir la nostra privacitat o no, com és l'exemple de Yahoo anteriorment mencionat, que l'única alternativa que ens oferia al no acceptar els nous termes d'ús (altament intrusius) era eliminar la nostra compta. Per exemplificar millor els petits matisos de les diferents polítiques que hem anat veient, ens servirem d'aquest apartat per fer la comparativa entre dues politiques situades en els dos extrems de la balança, per tal de mantenir la comparació neutral, compararem dos serveis -en aquest cas sistemes operatius-, els elegits seran els sistemes operatius Ubuntu i Microsoft Windows -més específicament, Windows 10-.

Hem d'anotar que aquestes polítiques acostumen a parlar més en nom de l'empresa que hi ha darrere que del producte en si oferit. Si fem una llegida en paral·lel d'ambdues polítiques, un dels primers punts de discrepància que trobem és la usabilitat dels serveis, mentre que Ubuntu en cap moment especifica que ens negarà l'accés a determinades característiques del sistema, mentre que Windows avisa que bastants dels seus productes requereixen certa informació obligatoria

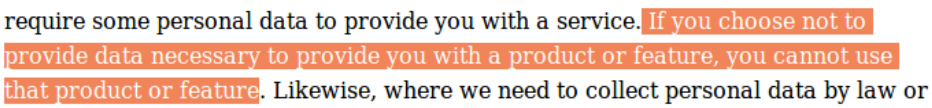

require some personal data to provide you with a service. If you choose not to provide data necessary to provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or

Figure 40: Usabilitat d'aplicacións en Microsoft Windows

Un punt que sí que veiem comú és en quines situacions aquestes empreses cediran la nostra informació, en ambdós casos la nostra informació personal quedarà relegada a aquelles ordres judicials que ho requereixin.

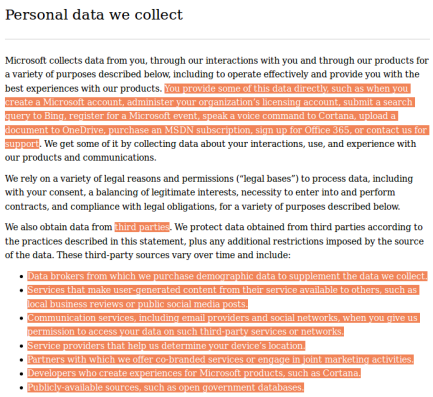

• Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
• Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
• Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
• Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms of use and other agreements; or to protect the rights, property, or safety of Canonical, our customers, or others.
In accordance with Privacy Notices made known at the time of collection.
In the event that we sell or buy any business or assets, in which case we will disclose your personal data to the prospective seller or buyer of such business or assets.
If Canonical or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.

Figure 41: En quines condicions l'informació personal pot ser cedida

Un aspecte important és quina informació en si els sistemes recolleixen, per al que fa Microsoft, enregistra tota aquella informació que li subministrem a qualsevol dels seus serveis, siguin cerques de Bing o qualsevol utilitat que tingui pel mig un dels seus serveis. El bloc que més crida l'atenció és

quina informació pot extreure de tercers i relacionar-la amb el nostre perfil, com és el cas de venedors d'informació o sense anar més enllà informació publica nostra que pot originar de bases de dades governamentals obertes.



Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

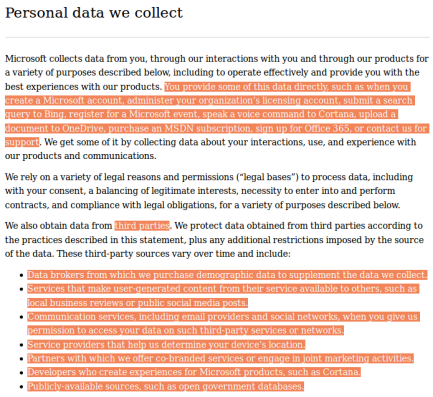
We rely on a variety of legal reasons and permissions ("legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.
- Service providers that help us determine your device's location.
- Partners with which we offer co-branded services or engage in joint marketing activities.
- Developers who create experiences for Microsoft products, such as Cortana.
- Publicly-available sources, such as open government databases.

Figure 42: Informació personal recollida per Windows

Per al que fa la informació personal recollida d'Ubuntu, aquesta s'engloba en informació que hem cedit voluntàriament al registrar-nos en algun dels seus serveis, també queda enregistrada la informació de les nostres visites a les pàgines que formin part de l'empresa, monitoritzant tota la metadada generada. Si Ubuntu aconsegueix informació nostra a partir de tercers i la relaciona amb el perfil d'usuari que tenim, aquest ens avisarà d'on l'ha extreta i que planeja fer amb ella, oferint una certa transparència.



Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions ("legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

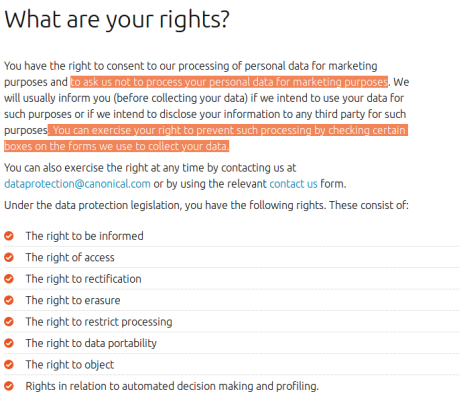
We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.
- Service providers that help us determine your device's location.
- Partners with which we offer co-branded services or engage in joint marketing activities.
- Developers who create experiences for Microsoft products, such as Cortana.
- Publicly-available sources, such as open government databases.

Figure 43: Informació personal recollida per Ubuntu

Un altre punt que trobem a faltar amb Windows és la menció dels nostres drets com a usuaris quan és la nostra informació la que canvia de mans, en tots els llocs on es menciona aquesta paraula

en la seva política de privacitat es refereixen als drets dels seus productes i els drets com a empresa, d'altra banda, podem trobar la llista dels nostres drets en el cas que no vulguem compartir la nostra informació amb terceres entitats.



What are your rights?

You have the right to consent to our processing of personal data for marketing purposes and to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data.

You can also exercise the right at any time by contacting us at dataprotection@canonical.com or by using the relevant contact us form.

Under the data protection legislation, you have the following rights. These consist of:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Figure 44: Drets d'Ubuntu

Com hem pogut veure, les polítiques de privacitat tenen un llenguatge formal i algunes pateixen de sobre-especificar obvietats mentre que alguns aspectes més obtusos queden amagats.

16 Guia de Bones pràctiques

16.1 Introducció

Un cop repassades totes les eines i serveis que tenim al nostre abast toca fer la selecció de quins són els serveis preferibles de cara a mantenir un perfil amb privacitat alta, per cada servei seleccionat també considerarem quines són les millors configuracions de cara a treure'n el màxim de les seves funcionalitats. Abans de començar farem l'incís en què, ja que la majoria d'utilitats que ofereixen més privacitat ho fan a canvi de L'experiència d'usuari (sigui perdent característiques o reduint la usabilitat), és a dir, tindrem en compte la balança que suposa guanyar anonimat amb la pèrdua de temps i esforços per garantir aquell mateix anonimat, això vol dir que moltes de les opcions seleccionades tindran un balanç entre seguretat i usabilitat, sense anar a cap extrem en cap dels dos casos.

16.2 Sistema operatiu

Com ja havíem comentat en les conclusions de l'apartat de SO's, la millor alternativa està en tenir un **sistema operatiu Linux** i a partir de quin sigui el nostre grau privacitat desitjat, podem baixar cap a distribucions més segures (Tails, Debian) o quedar-nos en aquelles que ens ofereixen una experiència d'usuari i una seguretat balancejades (Ubuntu, archLinux).

La nostra opció determinada serà un sistema Ubuntu gracies al seu balanç entre usabilitat i seguretat. Quan decidim començar la instal·lació en la nostra maquina, tenim la possibilitat d'encriptar la partició de disc que ocuparà Ubuntu. De no voler encriptar el disc en la seva totalitat, també podem tenir l'opció d'encriptar carpetes determinades a través del programa gnupg2. En un sistema Ubuntu acabat d'instal·lar, és important marcar quins són els privilegis de l'administrador i dels invitats. Una de les primeres coses a fer és denegar l'accés a programes que requereixin el superusuari a tots aquells usuaris que no siguin admin. Això ho podem aconseguir amb la següent comanda de terminal.

```
usuari@portatil:~$ sudo dpkg-statoverride --update --add root sudo 4750 /bin/su
```

Figure 45: Comanda d'Ubuntu

Per entendre que signifiquen els valors numèrics, hem de repassar els conceptes de permisos en fitxers de Linux [60], tenim tres grups d'usuaris: Propietaris, usuaris del mateix grup de privilegis i altres. També tenim tres tipus de permisos: Lectura, escriptura i execució, la combinació d'aquests permisos ens donarà una taula similar a aquesta:

- 0 : Sense permisos

- 1: Execució
- 2: Escriptura
- 3: Escriptura i Execució
- 4: Lectura
- 5: Lectura i Execució
- 6: Escriptura i Lectura
- 7: Escriptura, Lectura i Execució

L'ordre en què tinguem aquests dígits determinarà cada grup d'usuaris quins permisos té, el primer dígit en aquells permisos de 4 xifres és el de setuId, que canvia el comportament dels permisos de manera que aquests s'adaptin als del propietari i no als de l'usuari que ho haguí executat. Això denegarà completament L'accés al canvi de superusuari a tots els invitats. Si ara fem la prova des d'una altra sessió, veurem com se'ns prohibeix el pas.

```
guest-rwx1yb@portatil:~$ sudo
sudo: no s'ha pogut canvir el gid de l'usuari primari: L'operació no és permesa
sudo: unable to initialize policy plugin
```

Figure 46: Denegació d'accés

A més a més, també podem limitar l'accés al directori arrel de manera que només nosaltres tenim accés a la Home. Això s'aconsegueix amb la següent comanda.

```
usuari@portatil:~$ sudo chmod 0700 /home/username
```

Figure 47: Comanda d'Ubuntu

El valor de 700 significarà que l'administrador tindrà tots els permisos possibles mentre que els altres dos grups d'usuaris no tindran cap. En el cas que tinguéssim múltiples usuaris del mateix nivell a la nostra maquina, setejar el valor a 0750 permetria a aquests poder llegir i executar fitxers.

Paral·lelament, a part de les configuracions manuals en l'àmbit de fitxers que podem tenir en compte, les opcions natives de seguretat i privadesa d'Ubuntu també ens permeten adaptar segons quins paràmetres al nostre gust.

- Al apartat de diagnostics, podem desactivar l'enviament d'informes d'errors, tancant una posible fuita d'informació

- Podem desactviar també els resultats de cerca en línia al cercar en el tauler d'ubuntu
- de portes cap endins, al apartat de Fitxers i aplicacions podem desactivar l'enregistrament d'utilització de fitxers i aplicacions i fins i tot esborrar-lo completament per a que ningú sapiga quins son els fitxers accedits recentment al sistema
- Finalment, en l'apartat de seguretat podem obligar al sistema a demanar la contrasenya cada vegada que s'aturi temporalment el sistema o aquest estigui inactiu durant un determinat periode de temps.

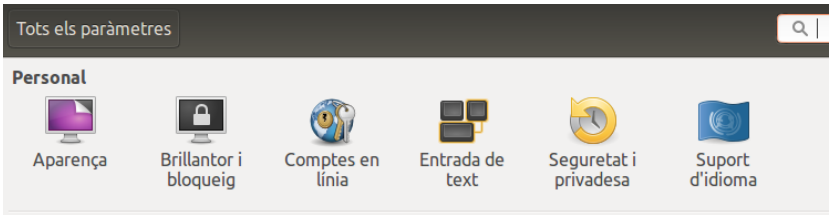


Figure 48: Paràmetres d'Ubuntu

Amb aquestes mesures preventives podem assegurar una certa millora en la seguretat del nostre equip i podem abordar altres fronts sabent que el sistema operatiu es trobarà protegit. Reiterant en el punt anterior, en el cas de voler mesures encara més fermes per la protecció de dades, podem provar altres distribucions especialitzades de la família Linux.

16.3 Xarxes

En l'apartat de xarxes considerem que tant l'opció d'una VPN com l'ús de TOR són valides. Per una banda tenim que les VPN no estan especialment relacionades amb el crim o l'anonimat, per l'altra tornem a la problemàtica que has de confiar en l'operador i això ens torna a ficar de la disjuntiva de la confiança de nou.

Vpn també serveix com a proxy, ja que les connexions procedeixen del servidor Vpn i no de l'usuari, en la Vpn el que passa dins es queda dins. Tor, alternativament, també ofereix uns nivells de privacitat extremadament alts, oferint-nos un anonimat gairebé total sempre que estiguem dintre de la seva xarxa de nodes canviants, l'unica problemàtica existent és dona quan aquest servei acostuma a alentir totes les comunicacions i ens marca com a un target que té alguna cosa a amagar.

D'aquesta manera, només ens queda determinar quin perfil d'usuari som i escollir quina de les dues opcions s'ajusta més a les nostres necessitats. Ja que hem considerat tenir en compte la usabilitat en aquesta equació la majoria de proteccions que necessitem es limiten a una capa més quotidiana

(missatgeria, navegació per pàgines licites, etc), **una VPN pot ser un servei més útil que TOR** i per tant aquesta sera la opció que estudiarem.

Abans de determinar un servei de VPN hem de fer passar les múltiples opcions oferides per diferents filtres en forma de preguntes. Ja que tenim una varietat tan extensa en serveis hem desenvolupar l'habilitat de discrimar-los a simple vista. Per tant, un bon servei de VPN ha d'assegurar uns mínims començant per la nostra identitat, no ha de voler saber res de nosaltres: Ja que el producte que es ven aquí és el de l'anonimat, ens ha d'estranyar si un servei VPN l'interessa saber de nosaltres, això també va enllaçat amb el tipus d'informació demanada a l'hora de donar-nos d'alta al servei, si ens demana informació que vagui més enllà de quin és el nostre correu ja ens està demanant massa.

També ha d'oferir un canvi automàtic d'IP periòdic i una destrucció de metadata constant per tal d'assegurar que el nostre perfil dintre d'aquella xarxa no es manté estàtic. Per al que fa l'àmbit monetari, no ha d'ser gratuït, el servei ha de justificar el seu preu i hem de dubtar seriosament de qualsevol servei Vpn que sigui gratuït. També hem de tenir en compte que ha d'estar en múltiples plataformes, de res ens serveix tenir una connexió privada en l'ordinador de casa si quan estem amb el telèfon mòbil no adoptem cap tipus de mesura preventiva. Per al que fa l'administració del servei, els seus servidors han d'estar allotjats en un País amb lleis compaginables amb la privacitat virtual que busquem, Holanda per exemple té una jurisdicció favorable de cara a la protecció d'informació virtual, aquesta recomanació sorgeix com que en altres països l'administració podria demanar totes les nostres dades al proveïdor VPN i depenent de la legislació aquest no podria fer res per negar-se.

Finalment, un cop tinguem en ment el nostre servei desitjat, aquest ha de superar el test de DNS. Podem fer una prova amb dnsleaktest.com [61] això ens permetrà saber quins són els servidors DNS que resolen les nostres peticions cada vegada que fem una petició HTTP, això permet als propietaris d'aquests serveis associar la nostra IP amb els llocs que visitem. Per a fer la prova, farem servir el servidor de DNS que tenim instal·lat al lloc de treball, primer farem passar el test sense connectar-nos a la Vpn i veure quins són els servidors que gestionen les nostres peticions:

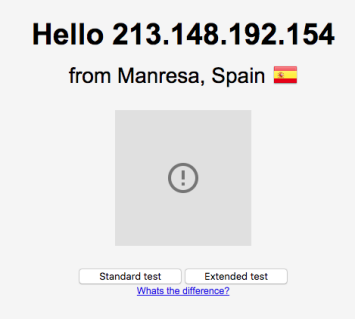


Figure 49: Pagina principal de DnsLeakTest

IP	Hostname	ISP	Country
74.125.181.11	none	Google	Belgium
74.125.47.8	none	Google	Belgium
74.125.73.71	none	Google	Belgium
74.125.73.88	none	Google	Belgium
74.125.181.6	none	Google	Belgium
74.125.47.139	none	Google	Belgium

Figure 50: Resultats DnsLeakTest

Com podem veure el nostre proveïdor de servei es Google i tots aquells servidors de DNS són els que resolen les nostres peticions i tenen la capacitat d'enregistrar tot el nostre tràfic i activitat en la xarxa, Així mateix, si fem la segona part de la prova veurem que un cop connectats a la Vpn això canvia dràsticament.

IP	Hostname	ISP	Country
23.215.61.17	a23-215-61-17.deploy.static.akamaitechnologies.com	Akamai Technologies	Netherlands
92.122.241.34	a92-122-241-34.deploy.static.akamaitechnologies.com	Akamai Technologies	Germany
23.215.61.19	a92-122-241-33.deploy.static.akamaitechnologies.com	Akamai Technologies	Netherlands
92.122.241.33	a23-215-61-19.deploy.static.akamaitechnologies.com	Akamai Technologies	Germany

Figure 51: Resultats DnsLeakTest 2

Ara podem veure que les nostres peticions queden resoltes per un altre servidor intermediari, amagant la nostra connexió completament de cara als servidors de Dns principals, com que tots els servidors de resolució són del proveïdor que tenim contractat es pot dir que ni hi ha cap fuita de xarxa en la nostra connexió privada, és per això que és important fer aquest test amb el nostre servei contractat com a últim pas per veure si realment es compleix el túnel de connexió privat.

Personalment, recomanem AirVPn [62] com a opció preferida gràcies a poder donar una resposta positiva a les qüestions anteriors i al conjunt de qualitats que presenta, tot i això qualsevol usuari pot escollir quin és el servei de VPN que més li convé amb una mica de recerca, aquest apartat tenia l'objectiu de desenvolupar el pensament crític de cara als serveis VPN per tal d'establir un estàndard de condicions mínimes d'un bon servei. Alternativament, sempre podem passar a l'ús de la xarxa TOR en el cas de voler una protecció més elevada.

16.4 Navegador

Considerem que **Firefox és la millor opció com a navegador** com que les altres opcions no han pogut acabar d'oferir un perfil de navegador que s'adeqües a la nostra cerca de privacitat. Tot i que la configuració per defecte de Mozilla Firefox ja ens és útil, podem prémer més per tal de millorar el servei jugant amb les seves funcionalitats.

Una funcionalitat que tenen tots els navegadors -inclòs firefox- és la de poder desar les contrasenyes introduïdes per estalviar-nos escriure-les el pròxim cop que entrem a la web, això, tot i ser útil, és un dels errors de seguretat activa més grans que com a usuaris podem permetre. Tenim dues maneres per controlar això, sigui no guardant mai les contrasenyes o tenir una contrasenya que estigui per sobre de totes les altres i que no estigui enregistrada enlloc.

És important tenir una contrasenya mestra per gestionar totes les contrasenyes guardades que tenim a l'ordinador, d'altra manera, estaríem posant en perill tot el conjunt de claus guardades a Firefox.

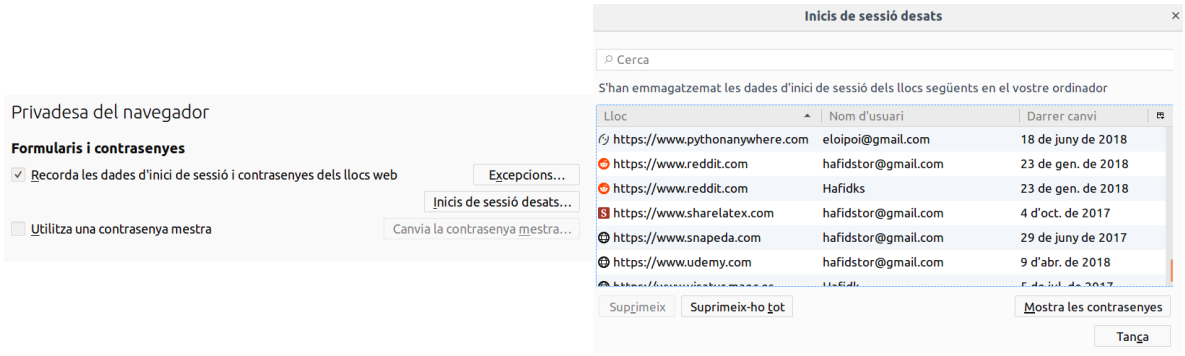


Figure 52: Password mestre i sessions desades a Firefox

Només faria falta que deixéssim el nostre terminal desatès durant un breu període de no més de 5 minuts i qualsevol individu podria fer-se amb totes les contrasenyes desades sense cap dificultat. Per evitar aquest escenari només hem de generar una clau que controli a totes aquestes claus.

D'entre els altres paràmetres per defecte que poden interessar-nos, trobem que podem fer una gestió automàtica de l'Historial i de les galetes, aconseguint que aquests s'esborrin sols al final de cada sessió. Si ens trobem amb necessitat de mantenir una galeta determinada, sempre podem afegir una excepció. Aquestes dues funcionalitats també és trobem de manera nativa al mode privat de Firefox.

També tenim la possibilitat de gestionar millor el tracking que rebem en navegar, ja sigui bloquejant trackers determinats (com podrien ser els de geolocalització de Google) o tallant per l'arrel i demanar a totes les pàgines que no ens segueixin.

Tot i que el llistat de paràmetres configurables per defecte de Mozilla Firefox ens semblen interes-

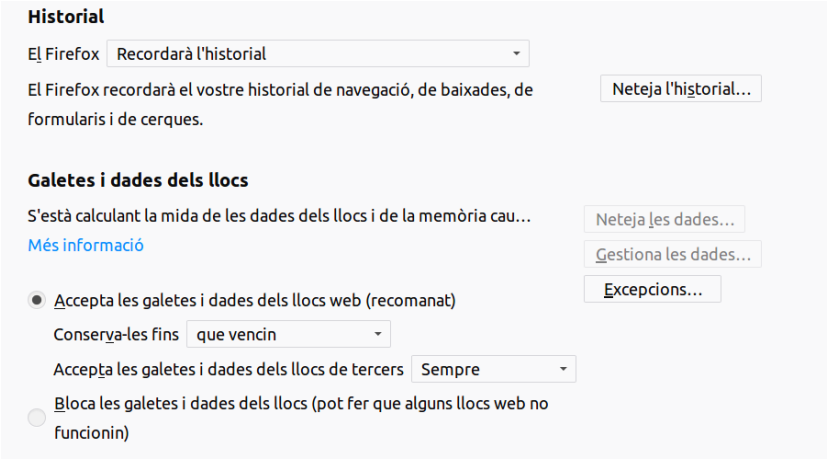


Figure 53: Paramàtres de privacitat de Mozilla Firefox

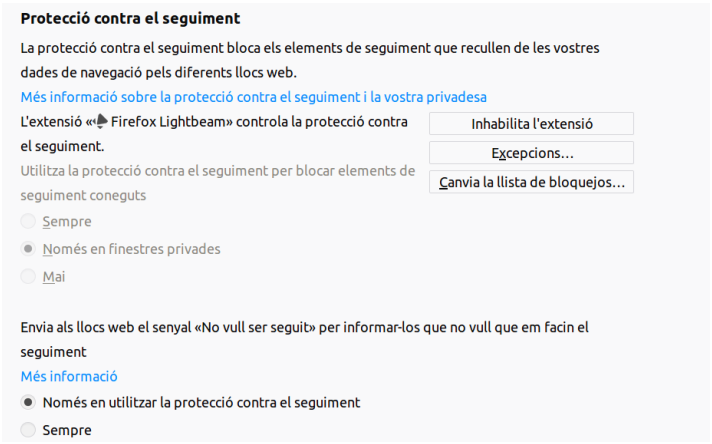


Figure 54: Més Paramàtres de privacitat de Mozilla Firefox

sants, podem baixar a un nivell més profund i accedir als paràmetres avançats de seguretat, per això només haurem d'escriure "about:config" en el cercador i el navegador ens avisarà de L'accés a aquesta zona.

Aquí trobarem un llarg llistat de paràmetres no disponibles en la pantalla de configuració. Per simplificar la feina i no analitzar tots els elements un per un, farem una repassada als que considerem més importants de cara a una navegació privada.

- privacy.firstparty.isolate Aquest paràmetre limita les cookies d'identificació a la pàgina en la qual estem, evitant que cookies d'anteriors pàgines puguin ser emmagatzemades i que puguem ser monitoritzats a través de diferents webs. D'aquesta manera, les cookies estaran aïllades les

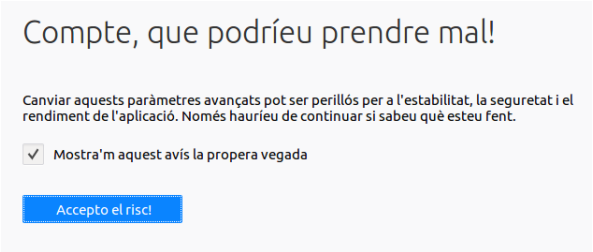


Figure 55: Warning dels paràmetres avançats

unes de les altres. Recalcar que de tots els paràmetres que introduirem, aquest és un dels que ens pot originar més conflictes a causa de la seva naturalesa [**?**]. El ficarem a True per activar la seva funcionalitat.

- privacy.resistFingerprinting Els nostres navegadors acostumen a donar més informació de la necessària, tal com el grandària de la pantalla, tipus de lletra ,zona horària, nuclis del sistema. Tota aquesta informació de miscel·lània pot semblar redundant, però si es combina en una sola entitat pot generar una empremta del nostre dispositiu, empenta que qualsevol pot reconèixer en la web. De fet, si utilitzem el servei de Amiunique.com [64] , ens oferirà la emprenta de paràmetres que cedeix el nostre navegador:

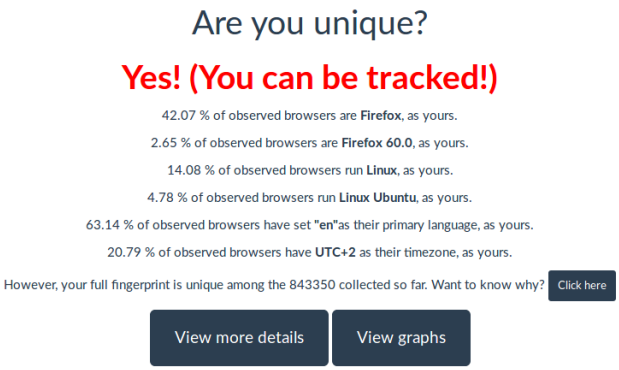


Figure 56: Emprenta generada

D'una xifra de 800000 sistemes que han passat pel test, el nostre sistema és únic, la seva configuració i combinació de paràmetres permet distingir-lo d'entre els altres, i per extensió el nostre dispositiu pot ser reconegut.

- `browser.send_pings` inhabilita la possibilitat de que les pagines visitades pugin trackejar els nostres clicks, aixo es degut a que al nou HTML5, els atributs de hiperlink poden tenir un

atribut de ping que fa POST cada vegada que el link es clicat, permeten a les pagines tenir una monitorització més constant [65].

- `browser.urlbar.speculativeConnect.enabled`, Aquest paràmetre ve donat a una nova funcionalitat de firefox, que pre-carregant les pàgines que l'autocompletat ens ofereix, tot i que en cap moment s'envia informació HTTP, aquest autocompletat si que fa que s'iniciïn les comunicacions per tal de tenir un petit increment en la velocitat de càrrega de les imatges [**?**].
- `dom.event.clipboardevents.enabled` notifica a les pàgines si l'usuari copia o enganxa qualsevol contingut d'aquesta, inclòs quin text en concret ha sigut copiat copiat [66].
- `browser.sessionstore.privacylevel`, Aquest paràmetre determina quanta informació queda enregistrada sobre la sessió actual (formularis, cookies i fins i tot posicions en les quals l'scroll es troba), tenim diferents nivells per setejar aquest valor, recomanem utilitzar el 2 per tal que mai es guardi informació extra [67].

Paralelament, també podem instalar extensions recomanades que fan una feina similar a la de activar i desactivar paràmetres de Firefox Peró resulten més còmodes d'utilitzar, d'entre aquestes extensions ens poden interessar les següents

- Https Everywhere: Re-escriu les peticions de xarxa de manera que ens obliga a entrar a la versió segura del protocol Http en totes les pàgines visitades
- Cookie AutoDelete: Elimina automàticament aquelles cookies que deixen de utilitzar-se (és a dir, cada cop que es tanca una pestanya).
- CanvasBlocker: Similar a la funcionalitat del paràmetre resistFingerprinting, redueix la quantitat de metadata generada.
- NoScript: Permet gestionar l'execució d'Scripts només en aquelles pàgines en les que confiem.

Com ja ha quedat demostrat una de le sprincipals fortalezes de Mozilla firefox és la capacitat d'oferir-nos tot un seguit d'opcions variades sense que ell determini que és lo millor per nosaltres. Amb les anteriors configuracions i algunes altres més extensions el nostre navegador quedara molt més protegit.

16.5 Buscador

El **buscador predilecte serà Startpage** de manera que combinat amb un Firefox ben configurat tindrem una millora significativa en la nostra navegació privada. Com que es tracta d'un servei web,

les opcions de privacitat poden ser una mica limitades, de totes maneres avaluàrem quines son les millors combinacions per guanyar marge en seguretat.

D'entre els paràmetres que ens poden interessar, trobem el de canviar el tipus de peticions de GET a POST, aquestes últimes per naturalesa no exposen la informació introduïda en els links. També tenim l'opció de permetre que el buscador ens avisi de quines són les pàgines que poden suposar un perill per a nosaltres. Si volem evitar completament accedir a les pàgines de reproducció de vídeos, Startpage ens permet veure'ls des de la seva pròpia interfície.

Ara bé, quan guardem aquests paràmetres ens assalta la pregunta d'on queda desada aquesta informació. La resposta més immediata ve donada en forma de cookie, però podem decidir generar una url que li ve donada un paràmetre generat que ens atorga la configuració desitjada. Poc més es pot dir en el camp del buscador, ja que no tenim la potestat de tocar més paràmetres de configuració seus.

16.6 Serveis de Missatgeria Web

El servei de missatgeria que hem decidit escollir com el més segur és **Protonmail**, servei dissenyat des de la base per enfocar uns principis fermes de privacitat i anonimat un dels beneficis d'utilitzar Protonmail és la ubicació dels seus servidors, aquests els trobem a Suïssa i estan protegits per les seves lleis de privacitat afegint també que gràcies a les regulacions europees actuals [**?**] que obliga als serveis d'aquesta naturalesa a adoptar un principi de privacitat per disseny.

Respecte a les seves opcions ofertades, ens podem trobar amb multitud de petites característiques escampades. Només al logejar-nos (o per defecte, en fallar el login i demanar un reseteig de password) Protonmail enviarà un codi de recuperació al mail secundari que li havíem indiciat, però amb l'avis que un cop resetejada la contrasenya també queden a zero les nostres claus d'encriptació, en altres paraules, perdem tots els missatges que teníem a menys que puguem recordar el primer password. Aquesta funcionalitat és especialment interessant per aquells casos on perdem l'accés del correu i un tercer es fa amb aquest, els nostres missatges antics estaran sempre segurs.

Com ja hem vist en altres serveis també tenim la possibilitat d'autentificar-nos en dos passos, duplicant la feina que hem de fer per entrar però també duplicant la seguretat.

Podem gestionar les sessions obertes en diferents navegadors, ja que ProtonMail ens donarà un històric de la data d'aquestes i el dispositiu, de voler-ho, podem forçar una desconnexió de totes aquelles sessions, i seguint amb l'històric, també tenim un llistat d'esdeveniments que ens dóna un resum de l'activitat, poden veure així si algun tercer ha intentat entrar al nostre dispositiu. Com podem veure, la majoria d'aquestes funcionalitats ofereixen a l'usuari un control dels accessos a la seva safata d'entrada, situació que els altres navegadors no havien tingut en compte o ho feien comprometent

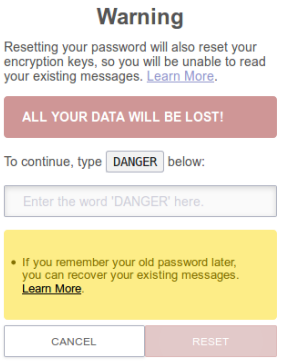


Figure 57: Reset de contrasenya a ProtonMail

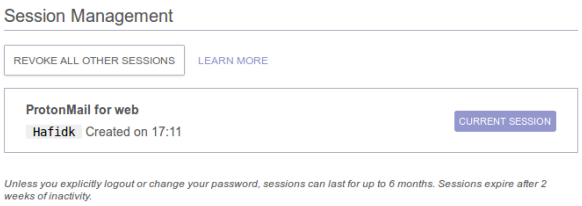


Figure 58: Gestió de sessións a ProtonMail

la nostra posició (per exemple els avisos de Google de si ens hem loguejat en una nova ubicació).

Ja que el quid de la qüestió en missatgeria web són les nostres claus, ProtonMail també ens ofereix la possibilitat de gestionar les nostres claus GPG RSA en el cas de que les vulguem utilitzar-les fora del servei.

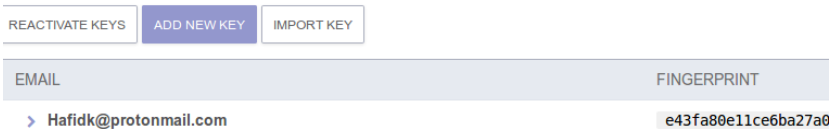


Figure 59: clau GPG a ProtonMail

Podem concloure que ProtonMail no només ofereix una seguretat elevada en les comunicacions entre usuaris sinó que a més també ofereix un seguit d'eines i possibilitats a l'usuari per gestionar la seva compta.

16.7 Serveis de Missatgeria mòbil

Seguint la conclusió a la que havíem arribat en l'apartat de sistemes de missatgeria mòbil, **l'opció preferida ha acabat essent Signal**, que ens ofereix uns avantatges en seguretat que les seves contraparts no han pogut superar.

Un dels primers passos que podem dur a terme de cara una comunicació més segura amb Signal és el mateix registre. Només instal·lar l'aplicació ja ens insta a introduir un número de telèfon per tal d'identificar-nos, podem considerar que aquesta no és una práctica gaire respectuosa de cara al nostre anonimat com que tercers poden triangular la nostra persona física amb l'usuari de Signal a través de telèfon (en la majoria de països, el número de telèfon va associat a una persona física). Signal és conscient d'aquesta situació i en el seu apartat de preguntes i respostes ens insta a introduir un número de telèfon al que tinguem accés però que no sigui nostre, només necessitem tenir-lo per al registre inicial, a més a més hem de registrar el número mitjançant SMS [69]per tal de mantenir aquell número de telèfon nostre i que cap altre usuari ens el sobreescrigui.

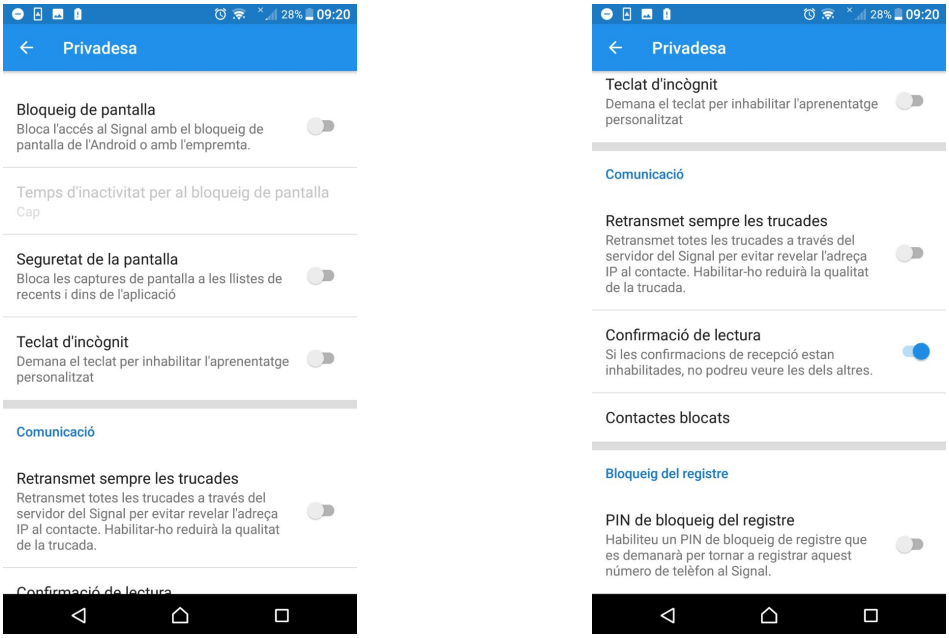


Figure 60: Opcions de privacitat a Signal

Un primer pas que podem seguir és desactivar completament les notificacions, tot i que perdrem aquesta útil funcionalitat, els missatges rebuts no apareixeran en un pop-up o en la pantalla de bloqueig. També és recomanable activar l'esborrat automàtic de missatges. En els servidors de Signal els missatges només queden emmagatzemats durant un breu període per tal d'assegurar-se de què han sigut entregats correctament i tot i això estan completament encriptats de manera que ni tan sols

l'administrador té accés al format de text pla. De manera que ens deixa amb l'escenari en què els continguts dels missatges només es troben en dos llocs: En el telèfon receptor i el nostre, de manera que si adoptem la bona costum d'esborrar-los constantment reduirem a la meitat la quantitat de llocs on es poden trobar aquests missatges.

Si volem utilitzar les funcionalitats de trucada i videotrucada, és recomanable fer-ho a través dels mateixos servidors de Signal, ja que d'aquesta manera el receptor no pot determinar la nostra adressa ip. Una molt bona practica consisteix en assegurar el número de seguretat dels nostres contactes físicament, per tal de reduir completament les possibilitats d'un "Man in the middle". Podem o bé quedar físicament amb la persona per tal d'escanejar el seu codi QR i verificar el seu usuari o enviar el conjunt de números per un altre canal de comunicació que no sigui Signal [68].

Aquestes són unes de les moltes opcions que ens ofereix Signal per millorar la nostra protecció, hem de contrastar el fet que un dels principals al·licients que fan aquesta l'opció guanyadora és el seu protocol de comunicació mentre que les altres característiques que hem esmentat són petits extres afegits.

16.8 Altres consells a tenir en compte

16.8.1 El perill de les xarxes publiques

Sota ningun concepte ens hem de conectar a una xarxa publica si no portem les proteccions indicades (ja sigui treballar amb una VPN o altres). Qualsevol paquet enviat dintre d'una d'aquestes xarxes gratuïtes pot esser interceptat per tercers, això es especialment perillós en les peticions POST de logueig ja que un cop iniciada la sessió, si que estem protegits i el trafic que enviem i rebem esta salvaguardat, Peró just abans de fer el logueig, la petició de POST que envia les dades d'usuari i la contrasenya no sol estar encriptada.

A més a més, en el cas de conectar-se sense més remei a aquestes xarxes, hem de veure de quin tipus son, donant prioritat a les WPA2 seguides per les WPA i finalment les WEP, aixo es degut a que la WP2 és L'estàndard actual i assegura una encriptació mínima en les seves comunicacions mentre que els altres protocols s'han quedat enrere tecnològicament.

16.8.2 L'importància del codi obert

Saber com funciona l'interior de qualsevol eina de seguretat que utilitzem és gairebé tan important que la tasca que determina aquesta. El codi obert ens permet asegurar-nos que l'aplicació fa realment el que diu sense segones intencions, tot i que un argument en contra d'aquest pot ser que el fa més insegur, això és completament falç, ja que precisament gràcies a què qualsevol usuari pot avisar d'errors

o forats de seguretat, aquest codi pot créixer i millorar la seva tasca, d'altra manera, no sabríem ni tan sols de l'existència d'aquest forat fins que no fos massa tard. És per això que la nostra recomanació és sempre donar prioritat a aquelles aplicacions i serveis que tinguin codi obert per sobre de les de codi privatiu.

16.8.3 Sistemes operatius Mobils

Com ja vàrem concloure en el seu moment, d'entre tots els sistemes operatius mòbils que tenim a l'abast actualment, el mal menor seria Android, decisió presa degut al flagrant monitoratge que fan altres sistemes com Iphone o WindowsPhone, tot i així aquesta opció està molt lluny de ser perfecta, en el cas que ens veiguem obligats a utilitzar el telèfon mòbil, una alternativa possible és instal·lar una distribució d'Android no oficial que estigui compromesa amb la nostra privacitat. En aquest cas la millor alternativa que podem recomanar és LineageOS, sistema operatiu mòbil de codi obert. No hem d'oblidar que instal·lar aquest sistema operatiu quedarà en paper mullat si decidim instal·lar funcionalitats dels serveis google, ja que li estarem donant a aquest accés i monitoratge del nostre dispositiu.

16.8.4 Serveis Google

Degut a la seva profunda penjada en l'internet actual, ens veiem obligats a dedicar un subapartat per avisar d'aquests serveis. Per una banda tenim el perill que suposa la seva monitorització massiva d'informació, per l'altra tenim que son serveis molt utils i acostumen a ser els més valorats d'entre la seva competència. Recomanar evitar en la seva totalitats aquests serveis pot esser complicat per la majoria d'usuaris ja que la majoria d'aquestes funcionalitats estan massa integrades en el nostre dia a dia per eliminar-les de cop, per tant, la nostra recomanació es basara en dossificar i descentralitzar l'ús d'aquests serveis, és a dir, per cada eina que utilitzem és millor que sigui en un servei que no utilitzem, d'aquesta manera evitem que tota la nostra informació i metadata caigui en un mateix lloc i sigui més facil identificar la nostra emprenta virtual.

16.8.5 Xarxes socials

Tal com varem avisar en el seu apartat, les xarxes socials suposen una fuga d'informació inacceptable per nosaltres, de manera que si ens veiem obligats al seu ús, reduiríem aquest únicament a Twitter, ja que dintre dels seus subalterns ha quedat demostrat que la seva política de privacitat i les s i els seus compromisos amb l'usuari son més alts que amb Facebook o Instagram, de totes maneres, queda a discreció de l'usuari la decisió final de si publicar a ulls de la xarxa el seu perfil.

17 Conclusions

Un cop finalitzat el projecte complert l'objectiu d'elaborar una guia que determina quines són les millors alternatives en l'entorn de privacitat a la xarxa, podem treure un seguit de conclusions determinants. Exposat el problema en totes les seves vessants i nivells, deduïm (contradictòriament amb la finalitat del treball) que és pràcticament impossible mantenir un nivell de privacitat absolut, malgrat això, una inversió de temps i un ús correcte de les eines adients poden marcar una diferència important amb la petjada generada. Addicionalment, també hem determinat que:

- Una inversió en privacitat sempre és inversament proporcional a la usabilitat, ja que o bé perdem funcionalitats o bé trobem passos intermedis necessaris pel camí.
- Es aconsellable desglossar els nostres serveis amb diferents proveïdors, buscant sempre un proveïdor diferent per cada necessitat que tinguem, d'aquesta manera aconseguim descompondre la imatge total del nostre perfil en petits esbossos que ens beneficien per mantenir un nivell d'anonimat elevat.
- És preferible utilitzar serveis que des de bon principi ens convencen, ja que fer el canvi més endavant és complicat.
- Remarcar la importància del codi obert, tal com hem anat veient al llarg de les diferents seccions, l'última línia de seguretat sempre és l'obertura del codi original, ja que sense aquesta mai tindrem una confiança total en les promeses del desenvolupador.
- Els perills més grans a l'anonimat som nosaltres mateixos, ja que en molts serveis és la nostra voluntat sense coaccions la que està d'acord en acceptar serveis que pregonen tot el contrari a una navegació privada.
- Tot i el llenguatge neutral i l'estil idèntic de les diferents polítiques de privacitat analitzades, hem pogut resoldre que l'únic aspecte interessant d'aquestes és el tipus d'informació recopilat, el diàmetre del cercle d'individus que tenen accés a ella, essent aquest últim clau per poder discriminar el grau de privacitat oferit per diferents serveis.

Possibles línies futures del projecte és centrarien en ampliar la quantitat de serveis analitzats per a solidificar encara més la conclusió respecte a quin servei és el més segur, també afegir que aquestes iteracions tindrien una vessant més pràctica, ja sigui demanant l'opinió pública en algunes qüestions o observar quin és el contingut dels paquets que viatgen per diferents xarxes i analitzar la seva possible triangulació al origen. Com a punt final, la conclusió més important a la que hem arribat és la necessitat

imperativa d'un sentit crític de cara a l'ús de les xarxes amb la importància d'adoptar una actitud seriosa respecte als nostres drets en aquestes i exigir als serveis utilitzats una transparència total i un compromís absolut amb l'anonimat. Al cap i a la fi, la informació dels usuaris té caràcter personal i intransferible i hem d'intentar viure amb aquesta premissa.

References

[1] Política de privacitat Windows

https://privacy.microsoft.com/en-gb/PrivacyStatement

[2] Política de privacitat d'Apple

https://www.apple.com/privacy/

[3] Política de privacitat Linux

https://www.linuxfoundation.org/privacy/

[4] Política de privacitat Linux

https://www.techradar.com/news/best-linux-distro-privacy-security

[5] Actualitzacions obligatòries Windows 10

https://arstechnica.com/information-technology/2015/07/
windows-10-updates-to-be-automatic-and-mandatory-for-home-users/

[6] Politica de privacitat Windows

https://www.apple.com/privacy/approach-to-privacy/

[7] Aplicacions inapropiades

https://www.telegraph.co.uk/technology/3358134/
Apples-Jobs-confirms-iPhone-kill-switch.html

[8] Intrusió en hardware de discs durs

https://www.macworld.com/article/3230498/storage/
apple-file-system-apfs-faq.html

[9] Bloqueig d'actualització de Telegram

https://www.theverge.com/2018/5/31/17412396/
telegram-apple-app-store-app-updates-russia

[10] Software-lock en reparacions no oficials.

https://motherboard.vice.com/en_us/article/
kbjm8e/iphone-7-home-button-unreplaceable-repair-software-lock

[11] Hardware privatiu a Windows

https://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/

[12] Intermediaris en la xarxa

http://www.yousubtitles.com/The-Future-of-Your-Personal-Data-Privacy-vs-Monetization-Stuart-Lacey-TEDxBermuda-id-459159

[13] Definició TOR

https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

[14] Funcionament xarxa TOR

https://geekytheory.com/que-es-y-como-funciona-la-red-tor

[15] Us de la xarxa TOR

https://lifehacker.com/what-is-tor-and-should-i-use-it-1527891029

[16] Necesitats dels usuaris a la xarxa

https://www.saporedicina.com/es/vpn-vs-proxy-vs-tor/

[17] Eines de protecció a la red

https://www.privateinternetaccess.com/pages/tor-vpn-proxy

[18] Perills d'un proxy

https://whatismyipaddress.com/proxy-risks

[19] Beneficis d'una VPN

https://whatismyipaddress.com/vpn

[20] 10 principis de la missió de transparència de Firefox

https://www.mozilla.org/~ca/about/manifesto/

[21] Situacions en les que hi ha tercers implicats

https://www.mozilla.org/~es-ES/privacy/

[22] Sincronització contes Mozilla

https://www.mozilla.org/~en-US/privacy/firefox/

[23] Navegació privada en firefox

https://support.mozilla.org/~es/kb/navegacion-privada-Firefox-no-guardar-historial-navegacion

[24] Política privacitat Google Chrome

https://www.google.es/~chrome/browser/privacy/

[25] Política privacitat Edge

https://privacy.microsoft.com/~en-us/windows-10-microsoft-edge-and-privacy

[26] Política privacitat Microsoft

https://privacy.microsoft.com/~en-us/privacystatement

[27] Política privacitat Google

https://www.google.com/~policies/privacy/

[28] Startpage i Ixquick

https://en.wikipedia.org/~wiki/Ixquick

[29] Politica de privacitat de Startpage

https://www.startpage.com/~esp/privacy-policy.html

[30] Politica de privacitat de DuckDuckGo

https://duckduckgo.com/~privacy

[31] Navegador Opera

https://en.wikipedia.org/wiki/Opera_(web_browser)

[32] Eines de privacitat a Opea

https://www.hongkiat.com/blog/reasons-to-use-opera-browser/

[33] Navegador Opera

https://www.opera.com/privacy

[34] Navegador Safari

https://ca.wikipedia.org/wiki/Safari_(navegador_web)

[35] Actualització de privacitat a Safari

https://www.wired.com/story/apple-safari-privacy-wwdc/

[36] Privacitat Yahoo

https://policies.yahoo.com/xa/en/yahoo/privacy/index.htm

[37] Fusió d'Oath i Yahoo

https://policies.yahoo.com/ie/es/yahoo/privacy/euoathnoticefaq/

[38] Metadades generalitzades

https://en.wikipedia.org/wiki/metadada

[39] Definició de Metadades
https://whatis.techtarget.com/definition/metadada

[40] GPG en diferents serveis
https://trendblog.net/encrypt-gmail-openpgp/

[41] Seguretat en Whatsapp
https://www.techadvisor.co.uk/feature/internet/
how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/

[42] Política Telegram
https://telegram.org/faq

[43] Encriptació i protocols de Telegram
https://core.telegram.org/mtproto

[44] Nivells de privacitat a Telegram
https://thehackernews.com/2016/08/hack-telegram-account.html

[45] Bots Telegram
https://core.telegram.org/bots

[46] Politica de privacitat Signal
https://signal.org/legal/

https://signal.org/legal/

[47] Beneficis de Signal
https://lifehacker.com/
secure-messaging-app-showdown-whatsapp-vs-signal-1794684943

[48] Guia d'ús Signal
https://www.popularmechanics.com/
technology/apps/a25736/signal-app-guide-how-to-use/

[49] Control de les nostres dades amb Google
/privacy.google.com/take-control.html

[50] Google y problemes amb privacitat
https://hackernoon.com/data-privacy-concerns-with-google-b946f2b7afea

[51] Gestió de dades esborrades

https://askleo.com/how-long-does-google-keep-my-account-information/

[52] Politica de Analytics

https://www.google.com.au/analytics/terms/us.html

[53] Conceptes de privacitat de google analytics

https://www.lovesdata.com/blog/2016/
what-you-need-to-know-about-google-analytics-and-privacy

[54] Extensió de LightBeam

https://addons.mozilla.org/ca/firefox/addon/lightbeam/

[55] Analisi de la falta de privacitat en les xarxes socials

https://www.sciencenews.org/blog/
scicurious/social-media-privacy-no-longer-personal-choice

[56] Política de privacitat Twitter

https://twitter.com/en/privacy

[57] Invasibilitat de Facebook

https://sites.google.com/site/cat200group5/home/invasive-privacy-agreements/2

[58] Intrusivitat de diferents xarxes socials

https://www.thebalancecareers.com/facebook-vs-twitter-privacy-issues-3515066

[59] Privacitat de dades a Instagram

https://help.instagram.com/519522125107875

PrivacitatInstagram

[60] Explicació dels permisos de Linux

https://help.ubuntu.com/community/FilePermissions

[61] Test de filtratge DNS

https://www.dnsleaktest.com/

[62] Pagina principal d'AirVPN

https://airvpn.org/

[63] Nivells tracking i parametres de Firefox per evitar-los.

https://www.ctrl.blog/entry/firefox-fpi

[64] Test IamUnique per determinar l'empremta del dispositiu.
https://amiunique.org/

[65] Documentació del parametre Send Pings
http://kb.mozillazine.org/Browser.send_pings

[66] Documentació del paramentre Clipboard
https://developer.mozilla.org/en-US/
docs/Mozilla/Preferences/Preference_reference/dom.event.clipboardevents.enabled

[67] Nivells de privacitat a Firefox
http://kb.mozillazine.org/Browser.sessionstore.privacy_level

[68] Beneficis d'ús de Signal
https://bdtechtalks.com/2018/01/29/
signal-how-to-make-the-most-out-of-one-of-the-most-secure-messaging-apps/

[69] Blocatge de registre en Signal
https://infosec-handbook.eu/blog/signal-myths/m2