Bezbednost na internetu podrazumevaju čuvanje privatnosti korisniku interneta.

Privatnost kao pojam podrazumeva čuvanje nekih ličnih informacija od drugih ili trećih lica.

Privatnost se obično definiše kao pravo svakog građanina da kontroliše svoje lične informacije i da odlučuje o njima (da ih čuva ili otkriva drugim licima). Privatnost je fundamentalno ljudsko pravo. Priznaju ga Univerzalna deklaracija o ljudskim pravima, Međunarodni sporazum o građanskim i političkim pravima i mnoge druge međunarodne i regionalne konvencije o ljudskim pravima.Može se reži da je privatnost korisnika narušena samom objavom bilo kojih informacija na društvenom web sajtu jer one automatski pripadaju kompaniji i ostaju sačuvane na njenim serverima čak i kada korisnik ugasi nalog. Takođe, ostavljanjem komentara na statusu "prijatelja", pro l korisnika koji je ostavio komentar postaje vidljiv ne samo prijateljima njegovog prijatelja nego i njihovim prijateljima.

Imajući u vidu da se većina, ako ne i sve društvene mreže, baziraju na ekonomskim principima poslovanja (omasovljavanje je logičan cilj), tehnička platforma društvenih mreža je tako koncipirana da od korisnika prikuplja određene podatke neophodne za upoznavanje i komunikaciju sa drugima (što je i suština društvenih mreža), ali ona isto tako prikuplja i određene podatke koji se ltriranjem segmentiraju i koriste u marketinške svrhe. Upravo ova mogućnost zloupotrebe određenih podataka od strane društvenih mreža predstavlja jedan od segmenata narušavanja privatnosti korisnika.

Nivoi privatnosti mogu se kategorisati na sledeći način:

1. **Lični podaci** - koje čivamo samo za lične potrebe
2. **Podaci koji se dele sa prijateljima koje mi biramo** - deklarisano deljenje
3. **Podatke koje mogu da vide i prijatelji naših prijatelja**
4. **Javni podaci** koje mogu da vide svi korisnici interneta.

Mada veoma je čest zaključak da korisnici interneta ustvari nemaju mogućnost zaštite podataka pri prenosu jer je ustvari transportni put javni pa svako ko ima naprednija znanja može da izvrši presretanje prenosa informacija na javnom transportnom putu komunikacije - Internetu.

Ako želimo veću bezbednost i čuvanje naših podataka onda svakako naša mreža ne sme biti

povezana na internet već to samo može biti mreža LAN - lokalnog tipa za interno deljenje sadržaja unutar mreže.

Zaštita privatnosti podrazumeva maskiranje i sakrivanje IP adresa, uvođenje dodatnih softvera za zaključavanje podataka, postavljanje jakih lozinki, ne objavljivanje svojih podataka i podataka sa svojim prijateljima jet time takođe prijateljima remetimo privatnost.

Jednostavno rečeno, ne želi svako da javno objavljuje detalje svog života na društvenim mrežama.

Takodje privatnost može biti poremećena instalacijom softvera na našem računaru koji ima tu namenu da prati naš rad i aktivnosti.

Takozvane, **HTTP- kolačići** (HTTP- cookie) koje se ubacuju u naš internet pretraživač i imaju različite funkcije od praćenja posećenih sadržaja, unešenih lozinki, brojeva kreditnih kartica do reklamiranja i izbacivanja reklamnih sardžaja u naš internet pregledač. One pored lokalnog praćenja sardžaje mogu da ostavljaju na servere odakle su instalirane čime bitni podaci ostaju na serverima van našeg dometa. Kolačići, mogim ljudima koji ne razumeju olakšavaju rad time što su im zapamćene lozinke i vrši se automatska popuna u formi za pristup sajtu.

Fleš kolačići rade na sličnom principu samo uz pomoć programa koji se zove Adobe Flesh player čuvajući informacije na našem računaru.

Stalni kolačići instaliraju se trajno u računaru pomoću java-script programa i otporni su na brisanje jer sami sebe kopiraju i menjaju ekstenzije (programi Flash Local Share Object, razni HTML5 ehanizmi praćenja i čuvanja podataka)

Internet pretraživači i provajderi, uvek moraju da pošalju našu IP adresu čime se otkriva naša lokacija serveru kojem pristupamo, jednostavno rečeno Internet tako radi mora da se zna ko zahteva a ako odgovara na zahtev. Tako da naše aktivnosti pamti server provajdera, što automatski daje povratne informacije ko je i šta radio po netu.

Ulazni podaci pri logovanju na operativni sistem, takodje mogu biti još jedan od izvora informacija o korisniku računara. Naravno u istraživačkim centrima i privatnim kompanijama gde se rarzvijaju aplikacije to je obavezna kontrola rada radnika na računaru za čije podatke odgovara kompanija jer je radnik tada pod ugovorom sa kompanijom.

Legalne opasnosti spadaju u dozvoljene tehnike prikupljanja podataaka o korisnicima Interneta za potrebe statističkih istraživanja i marketinga.

Prateći odluku EU saveta ministara u Briselu , januara 2009 , ministarstvo unutrašnjih poslova Velike Britanije (engl. *Home Office*) je prihvatio plan da se policiji dozvoli pristup sadržaju na računaru pojedinca bez sudskog naloga. Proces pod nazivom „daljinsko pretraživanje“ je omogućavao jednoj strani da, sa udaljene lokacije, pregleda tuđi tvrdi disk i internet saobraćaj, uključujući imejl, istoriju pretraživanja i posećene stranice. Policiji iz EU je sada dozvoljeno da zatraže od britanske policije da sprovedu daljinsko pretraživanje umesto njih. Istraživanje može biti odobreno i pronađen materijal predat i korišćen kao dokaz na osnovu sumnje nadređenog komandanta koji je smatrao da je ovakav postupak bio neophodan radi sprečavanja ozbiljnog prestupa. Opozicija MP i civilni liberali su zabrinuti da se ovakvi postupci kreću u smeru širenja nadzora i predstavljaju pretnju po ličnu privatnost. Šami Čakrabarti (engl. *Shami Chakrabarti*), direktor grupe boraca za ljudska prava Sloboda, kaže: „Javnost će želeti da to bude pod kontrolom novog zakonodavstva i sudske autorizacije. Bez tih garancija ovo je razorni udarac po bilo koji aspekt lične privatnosti“.

FBI-ov softverski program Čarobni fenjer (engl. *Magic Lantern*) je bio tema mnogih debata kada je iznesen u javnost 2001 . godine. Čarobni fenjer je program " trojanac " koji pamti korisnikove otkucaje na tastaturi čineći šifrovanje bespotrebnim. [19]

Drugi potencijalni rizici po privatnost na internetu

- Malver (engl. *Malware*) je skraćeni termin za termin zlokoban softver i koristi se prilikom opisa softvera koji čini štetu računaru, serveru , ili mreži računara, bilo da je to preko virusa , trojanca, spajvera... [20]

- Spajver (engl. *Spyware*) je deo softvera koji dobija informacije sa korisnikovog računara bez njegove saglasnosti.
- Veb buba (bag) je ugrađena u veb stranicu ili imejl i uglavnom je nevidljiva posetiocu stranice ili čitaocu imejla. Ona omogućava proveravanje da li je osoba posetila neku konkretnu stranicu ili pročitala konkretnu imejl poruku.
- Fišing (engl. *Phishing*) je krivično delo pokušaja pridobijanja zaštićenih informacija poput korisničkog imena, lozinke, kreditne kartice ili informacija iz banke. Ovo je proces internet kriminala u kom se neko preruši u lice od poverenja u nekom obliku elektronske komunikacije.

- Farming (engl. *Pharming*) je pokušaj hakera da preusmeri saobraćaj sa legitimne veb stranice na potpuno drugačiju internet adresu. Farming se može izvesti promenom fajla domaćina na kompjuteru žrtve ili iskorišćavanjem slabosti na DNS serveru .