dataskydd.net
ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Finansdepartementet
103 33 Stockholm

Falun 2017-07-26

Remissyttrande över SOU 2017:30 (Fi2017/01644/OU) – En omreglerad spelmarknad

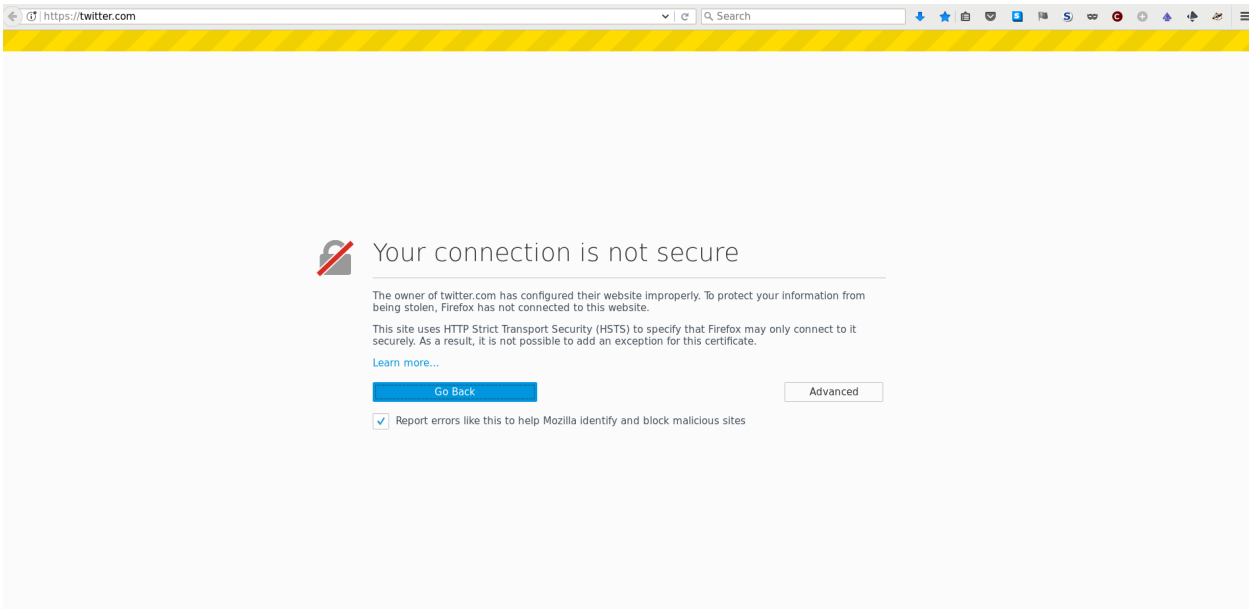
Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige.

Förslag

Varningsskyltar är en säkerhetsrisk (avstyrker förslag i kap. 24.11.8)
Vi avstyrker utredningens förslag att internetleverantörer ska vara skyldiga att på uppmaning av Spelmyndigheten upprätta ett varningsmeddelande för domänadresser som erbjuder spel utan licens i Sverige. Den tekniska procedur som behövs för att visa varningsmeddelandena kan hamna i konflikt med nya säkerhetsåtgärder i webbläsare som bland annat skyddar privatpersoner och konsumenter från nätfiske, identitetsstöld och spionmjukvaror, och vi anser att säkerhetsåtgärder som skyddar webbanvändare är ett tyngre intresse än statens intresse av att visa varningsskyltar.
Kontraproduktiv personuppgiftsreglering (avstyrker förslag Spellag, kap. 17)
Vi avstyrker förslagen om personuppgiftsreglering i Spellagens 17 kapitel. Förslagen riskerar att lura både Spelmyndigheten och spelföretag att tro att de inte har ett ansvar att göra konsekvensbedömningar avseende dataskydd eller vidta lämpliga tekniska och organisatoriska åtgärder, eftersom den specifika detaljreglering som föreslås får det att framstå som om att utredaren redan gjort sådana bedömningar.

Varningsskyltarna är en säkerhetsrisk

Användares säkerhet i nätmiljöer har blivit ett ökat fokus för näringslivet under det senaste decenniet. Särskilt har flera anglosaxiska länders lagstiftning om tvingande transparens kring säkerhetsproblem gentemot konsumenter gjort det lättare för slutanvändare att utkräva ansvar och få reda på något gått fel. Därför



Figur 1: Så här kan det se ut när webbläsaren upptäcker att en teleoperatör (i detta fallet på ett kollektivt färdmedel med gratis uppkoppling för passagerare) försöker rikta om webbanvändarens försök att nå en HSTS-konfigurerad webbplats till en av teleoperatören vald webbplats.

Bild: Screenshot från en Mozilla Firefox-webbläsare.

har området användbar säker (usable security) blivit ett stort forskningsfält.[1]

En konsekvens av att fler forskare och företag på allvar börjat lägga pengar på utredningar av hur webbanvändare typiskt sett interagerar med olika säkerhetsfunktionaliteter i mjukvaror är att man har insett att de tidigare metoderna för att skydda webbanvändare var ineffektiva. Till exempel är det inte ovanligt att webbanvändare kringgår meddelanden som varnar dem för att de är utsatta för en risk att hamna på ett bedräglig webbsida, eller en webbsida som innehåller farlig kod.[2]

Vidare har det länge varit känt att hela webbens system för säker kommunikation, de kryptografiska protokollen SSL/TLS tillsammans med systemet för digitala (kryptografiska) certifikat, inte varit fullgott trygga för konsumenter. Bland annat har det varit möjligt för stater att tvinga teleoperatörer att kapa trafiken mellan kända sociala nätverk och slutanvändare, på ett sådant sätt att man kunnat spåra dissidenter och deras familjer, eller helt enkelt stjäla deras sociala media-identiteter.[3]

Det har också varit möjligt för certifikatutfärdare, som ansvarar för att krypteringscertifikat finns tillgängliga för de webbplatser som vill garantera säker kommunikation för sina användare, att utfärda samma certifikat flera gånger till olika aktörer. Det är givetvis inte tillåtet, men det har hänt flertalet gånger.[4] Certifikatutfärdarna som en vanlig webbläsare litar på utgörs av hundratals olika företag och institutioner runtom i världen. Det har inneburit att webbanvända-

[1] Lorrie Cranor, professor vid Carnegie Mellon University, är världsledande på området användbar säkerhet för slutkonsumenter. Hennes forskning finns tillgänglig på hennes webbplats: http://lorrie.cranor.org/. Det har emellertid också uppstått ett antal årligen återkommande konferenser på området användbar säkerhet, bland annat USENIX Enigma och EuroUSEC. De är lätta att söka upp på webben.

[2] *Se t. ex.* Emily Schechters (Google Security UX) presentation Inside "MOAR TLS:" How We Think about Encouraging External HTTPS Adoption on the Web på USENIX Enigma 2017.

[3] *Se t. ex.* Danny O'Brien, CPJ Internet Advocacy Coordinator, Tunisia invades, censors Facebook, other accounts, 5 januari 2011.

[4] Webbplatsen SSLMate har upprättat en lista över händelser som regelbundet uppdateras: https://sslmate.com/blog/post/history_of_ca_sanctions men en detaljerad beskrivning av en nylig händelse (sommaren 2017) finns också i Ars Technica (20 juli 2017) Google drops the boom on WoSign, StartCom certs for good.

re kunnat luras att de besöker en legitim webbplats som är säker, när de i själva verket besöker en osäker webbplats som försöker lura dem.

En lösning på det första problemet är en standard som heter HTTP Strict Transport Security (HSTS).[5] Det är ett sätt att tala om för webbläsaren att alltid använda krypterade anslutningar (HTTPS) vid kommunikation med en viss webbplats. Om en teleoperatör försöker kapa trafiken till en webbplats som webbläsaren vet använder HSTS får besökaren upp en varningssida om att någon kanske försöker kapa trafiken.

Det andra problemet - med falska certifikat - är mycket mer ovanligt, eftersom certifikatutfärdare som ertappas med sådant kastas ut från den samling certifikatutfärdare en webbläsare litar på. Det finns emellertid en lösning även på det problemet: HTTP Public Key Pinning (HPKP).[6] Det innebär att ett visst krypteringscertifikat låses till en viss domän. Om en teleoperatör då försöker kapa trafiken till och från en viss webbplats och skicka den till en annan webbplats, får webbanvändaren en varning från sin webbläsare om att någon försöker kapa trafiken och utsätta den för en säkerhetsrisk.

Dataskydd.net har rekommenderat svenska kommuner att använda sig av HSTS för att se till att all trafik alltid är krypterad och för att undvika vissa typer av attacker.[7]

Utredarens förslag innebär emellertid att webbanvändare ska skickas vidare från en lista av webbplatser som Spelmyndigheten har bestämt till en särskild varningssida, på ett sätt som eventuellt strider mot de här nya säkerhetsfunktionerna i webbläsare.

Detta kommer för det första inte att gå, i fall webbplatsen i fråga använder HSTS (vilket är trivialt att implementera), eftersom webbläsaren kommer att berätta för webbanvändaren att någon försöker kapa dennes trafik. I alla fall om det olicensierade spelbolaget ändå är tillräckligt seriöst för att ta sina legitima konsumenters (så som konsumenter i andra länders) intressen på allvar.

Men för det andra kommer Spelmyndigheten få ett institutionellt intresse av att motarbeta starkare säkerhetsmekanismer för webbanvändare på spelsajter, eftersom de säkerhetsskapande åtgärderna gör Spelmyndighetens åtgärder mot i Sverige olicensierade spel meningslösa. Det är dåligt för alla webbanvändare i hela världen, även de som inte besöker spelsajter.

Särskilt beklagligt är ovanstående mot bakgrund av att teleoperatörerna tydligen försökt förklara för utredaren att dennes förslag är tekniskt olämpliga.[8] Men även om utredaren inte fann att teleoperatörerna var tillräckligt övertygande, eller om dessa inte på ett rättvisande sätt kunnat representera utvecklingen av användarvänlig säkerhet i webbläsare (eftersom teleoperatörer inte utvecklar webbläsare), så har utredaren ändå slarvat.

Utredaren borde ha tillfrågat en bredare mängd aktörer, till exempel sådana

[5] IETF, RFC 6797, HTTP Strict Transport Security (HSTS).

[6] IETF, RFC 7469, Public Key Pinning Extension for HTTP.

[7] *Se t. ex.* Kommunundersökningen, om dataskyddsnivåerna på svenska kommuners webbplatser: `https://dataskydd.net/kommuner/` eller verktyget Webbkoll, som mäter dataskydd på webbplatser: `https://webbkoll.dataskydd.net`

[8] SOU 2017:30, del 2, s. 144:

> *Utredningen har också haft ett möte med företrädare för IT- och telekombranschen och diskuterat, som ett alternativ till IP-blockering, minde ingripande åtgärder som t.ex. en varningstext med information om att denna sida inte står under svensk tillsyn eller har en licens i Sverige. Företrädaren för IT- och telekombranschen menar dock att det är samma principiella problematik med en varningstext som med IP-blockering.*

som är aktiva inom utveckling av säkerhetsfunktioner för webben och utveckling av webbläsare, innan han föreslog åtgärden med varningsskyltar.

Personuppgiftsregleringen som föreslås kontraproduktiv

Dataskydd.net rekommenderade utredaren inte att göra särskilda bestämmelser om personuppgiftshantering i spellagen, eftersom den verksamhet som personuppgifterna samlas in för redan bör vara tillräckligt tydlig reglerad i lagstiftningen för att spelföretagen och tillhörande myndigheter ska kunna tillämpa EU:s dataskyddsförordning direkt.[9]

Utredaren verkar ha tagit till sig budskapet att konsekvensanalyser avseende dataskydd kan göras av någon annan än utredaren, men tyvärr på ett sätt som inte varit bäst hjälpsamt för vare sig myndigheter, företag eller privatpersoner. De bristande konsekvensanalyserna har också tagits upp av Datainspektionen i deras remissyttrande.[10]

PERSONUPPGIFTSANSVARET för spelföretagen behöver förmodligen inte lagstadgas i Spellag 17 kap. 4 § eftersom det är uppenbart att de blir personuppgiftsansvariga när de skriver avtal med kunden. Personuppgiftsansvaret för Spelmyndigheten behöver inte heller lagstadgas eftersom det är uppenbart att de är ansvariga för personuppgifter de behandlar som en del i att fullfölja sina juridiska förpliktelser.

ALLA BEHANDLINGSGRUNDER som förslås av utredaren i Spellag 17 kap. 5 § följer av de uppgifter som Spelmyndigheten tilldelas i andra lagparagrafer i den föreslagna spellagen. Eftersom artikel 6.1.c i EU:s allmänna dataskyddsförordning redan medger att man behandlar uppgifter när det krävs för att man ska uppfylla en juridisk förpliktelse är bestämmelsen överflödig. I värsta fall kan den föreslagna specialregleringen lura Spelmyndigheten att den inte behöver göra konsekvensanalyser avseende dataskydd[11] eller vidta andra åtgärder som dataskyddsförordningen kräver för att säkerställa insyn, information till enskilda, datasäkerhet och vettigt utformade organisatoriska rutiner.[12]

Artikel 6.1.c:
Behandling är endast laglig om [den] är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

ALLA BEHANDLINGSGRUNDER som föreslås av utredaren i Spellag 17 kap. 6 § följer av de uppgifter som spelföretagen tilldelas i andra lagparagrafer. Eftersom artikel 6.1.c i EU:s allmänna dataskyddsförordning redan medger att man behandlar uppgifter när det krävs för att man ska uppfylla en juridisk förpliktelse är bestämmelsen överflödig. I värsta fall den föreslagna specialregleringen

[9] Dataskydd.net:s skrivelse till utredningen om en ny spellicenslag, våren 2016.
Dataskydd.net ser inte att det behövs särskilda undantag från dataskyddslagstiftningen för att uppnå utredningens mål. Vi förordar en tydlig definition av vad "spelansvarsåtgärder" är, så att speltjänstleverantörer kan tillämpa dataskyddsförordningens vanliga principer och regler vid utformandet av dessa åtgärder.

[10] Datainspektionen, Dnr 1015-2017, 21 juni 2017.
Datainspektionen avstyrker de förslag som innebär behandling av personuppgifter, främst mot bakgrund av att betänkandet inte innehåller någon egentlig utredning och analys av förslagens inverkan på enskildas personliga integritet och därför inte kan anses uppfylla de krav som följer av dataskyddsförordningen1 och regeringsformen.

[11] Förordning, 679/2016, artikel 35 (*Konsekvensbedömning avseende dataskydd*).
[12] Förordning, 679/2016, Kapitel III (*Den registrerades rättigheter*) och Kapitel IV (*Personuppgiftsansvarig och personuppgiftsbiträde*).

lura spelföretagen att de inte behöver göra konsekvensanalyser avseende dataskydd[13] eller vidta andra åtgärder som dataskyddsförordningen kräver för att säkerställa insyn, information till enskilda, datasäkerhet och vettigt utformade organisatoriska rutiner.[14]

Om utredaren till exempel avsåg att begränsa spelföretagens möjligheter att rikta reklam mot enskilda användare hade det varit bättre att helt enkelt begränsa spelföretagens möjligheter att rikta reklam mot enskilda användare genom en marknadsföringsbestämmelse.

Utredaren borde alltså ha fokuserat på *vilka verksamheter* och *vilka arbetsuppgifter och förpliktelser* Spelmyndigheten och spelföretagen ska genomföra och tilldelas, snarare än försöka reglera personuppgiftshanteringen. Bestämmelser om dataminimering, ändamålsbegränsning, lagringsminimering och användares rättigheter skapar ett system där spelkonsumenterna själva, förhoppningsvis, ges tillräckliga verktyg av lagstiftaren för att upprätthålla sina rättigheter inom varje verksamhet. Detaljreglering av uppgiftskategorierna lämnas hellre till föreskrifter från Datainspektionen, om en sådan alls borde göras.

Systematiken i den europeiska dataskyddslagstiftningen som Spellag 17 kap. är tänkt att komplettera är att företag och myndigheter ska vara tillräckligt transparenta och ge tillräckligt mycket insyn för att medborgare, konsumenter och ideella föreningar ska kunna utkräva eget ansvar av myndigheter och företag.[15]

Det antyds i utredarens förslag till Spellag 17 kap. 7 § att man velat begränsa ändamålen med uppgiftsbehandlingen på sådant sätt att dessa inte inkluderar marknadsföring. Men varför i sådana fall inte bara besluta att spelföretag inte får ägna sig åt (demografiskt) riktad marknadsföring? Det blir otydligt får både konsumenter, företag och tillsynsmyndigheter ifall utredaren, och därmed även regeringen, inte är tydliga med vad de vill att var och en av parterna ska göra. Dataskyddslagstiftningen ska inte användas som bakväg för att tvinga igenom restriktioner av marknadsföringsåtgärder, på samma sätt som reglerna för marknadsföringsåtgärder inte ska vara en bakväg för sämre dataskydd.

ONÖDIG DUBBELLAGSTIFTNING skapas genom den av utredaren föreslagna Spellag 17 kap. 7 §, som redan följer av EU:s allmänna dataskyddsförordning Art 5.1.c (*dataminimering*). Det är oklart varför utredaren finner det lämpligt att åsidosätta dataskyddsförordningens likalydande bestämmelse.

Detsamma gäller de av utredaren föreslagna Spellag 17 kap. 11–12 §§, som har sina motsvarigheter i EU:s allmänna dataskyddsförordning artikel 5.1.f (*integritet och konfidentalitet*), artikel 25 (*inbyggt integritetsskydd*), och artikel 5.1.e (*lagringsminimering*). Genom att snickra ihop egna bestämmelser som avviker från eller kanske till och med dubblerar den allmänna dataskyddsförordningens bestämmelser gör utredaren det svårare för Datainspektionen att utöva tillsyn och utfärda föreskrifter för verksamheterna på både Spelmyndigheten och hos spelföretagen. Utredarens förslag är till exempel inte på något vis tekniskt bättre, tryggare eller säkrare för spelare och medborgare än vad Datainspektionens redan befintliga riktlinjer för inbyggt integritetsskydd är.[16]

BESTÄMMELSEN som föreslås i Spellag 17 kap. 8 § är onödig eftersom det inte är uppenbart hur några av syftena listade i 5–6 §§ kräver behandling av känsliga personuppgifter. Regler om detta borde lämnas till föreskrifter, eller om det är absolut nödvändigt och sker noggranna konsekvensbedömningar avseende dataskydd, till en förordning.

Lagstiftade undantag från dataskyddet ska alltså normalt vara proportionerligt, strikt nödvändigt och faktiskt svara mot mål av allmänt samhällsintresse,[17]

[13] Se fotnot 11.

[14] Se fotnot 12.

[15] För ett längre resonemang om hur ideella föreningar kan vara hjälpsamma i att bevaka just personuppgiftshantering hos företag och myndigheter, se Dataskydd.net:s förklaring av den franska konsumentorganisationen Que Choisirs kampanj i vårt remissyttrande över SOU 2017:29, Brottsdatalag.

[16] Datainspektionen. Inbyggt integritetsskydd, 2012.

[17] EU:s stadga för grundläggande rättigheter (2010/C 83/02), artikel 52.

inte vara något som man spekulerar i för att man inte vet vad man håller på med.

I sak utgör bestämmelsen också en onödig detaljreglering av användargränssnitt som inte gör något för att skydda den personliga integriteten, men skapar sämre förutsättningar att anpassa tekniska lösningar efter nya säkerhets- och dataskyddsteknologier. Dataskydd.net tog upp detta i sin inlaga till utredningen.[18]

De förslag som läggs till Spellag 17 kap. 9–10 §§ är klart onödiga mot bakgrund av förslaget om en ny brottsdatalag. Även om vi sympatiserar med utredarens svåra sits, då tiotalet personuppgiftsutredningar varav flera föreslår ramlagar pågått samtidigt, känns det som att sådana här specialregler intuitivt bara är onödiga. Då har man missat att lagstiftningskroppen som helhet behöver ha någon systematik.

Amelia Andersdotter
Ordförande, Dataskydd.net

[18] Se ovan fotnot 9.

Källhänvisningar med länkar där möjligt

1. Ars Technica (20 juli 2017) Google drops the boom on WoSign, StartCom certs for good. https://arstechnica.com/information-technology/2017/07/google-drops-the-boom-on-wosign-startcom-certs-for-good/
2. Lorrie Cranor, professor vid Carnegie Mellon University, är världsledande på området användbar säkerhet för slutkonsumenter. Hennes forskning finns tillgänglig på hennes webbplats: http://lorrie.cranor.org/
3. Datainspektionen. Inbyggt integritetsskydd, 2012. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/
4. Datainspektionen, Dnr 1015-2017, En omreglerad spelmarknad (SOU 2017:30), 21 juni 2017. http://www.datainspektionen.se/Documents/remissvar/2017-06-21-yttrande-spelreglering.pdf
5. Internet Engineering Task Force (IETF), RFC 6797, HTTP Strict Transport Security (HSTS). https://tools.ietf.org/html/rfc6797
6. Internet Engineering Task Force (IETF)„ RFC 7469, Public Key Pinning Extension for HTTP. https://tools.ietf.org/html/rfc7469
7. Danny O'Brien, CPJ Internet Advocacy Coordinator, Tunisia invades, censors Facebook, other accounts, 5 januari 2011. https://cpj.org/blog/2011/01/tunisia-invades-censors-facebook-other-accounts.php
8. Emily Schechters (Google Security UX) presentation Inside "MOAR TLS:" How We Think about Encouraging External HTTPS Adoption on the Web. https://www.usenix.org/conference/enigma2017/conference-program/presentation/schechter
9. SSLMate:s lista över tillfällen då certifikatutfärdare slarvat med att hålla rätt på hur de utfärdar certifikat på ett för webbsäkerheten menligt sätt: https://sslmate.com/blog/post/history_of_ca_sanctions