Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)6 5438 6680
E ot.vandaalen@bof.nl
W www.bof.nl

Bankrekening 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Aan de leden van de
Commissie Veiligheid en Justitie

Betreft
Input Bits of Freedom over kabinetsstandpunt gegevensverwerking en -bescherming

Datum
Amsterdam, 12 september 2011

Geachte heer, mevrouw,

1. Op 15 september 2011 zal de Commissie Veiligheid en Justitie de notitie van de Teeven over gegevensverwerking en -bescherming bespreken. Bits of Freedom verdedigt de grondrechten op privacy en communicatievrijheid op internet. Zij maakt graag van de gelegenheid gebruik om een aantal aandachtspunten met u te delen. Zij beperkt zich vooral tot haar eigen expertise, internetprivacy, en gaat niet in op andere onderwerpen, zoals ANPR:

    - Privacybescherming wordt steeds belangrijker in onze maatschappij. Privacy-inbreuken hebben tot gevolg dat het vertrouwen in online diensten afneemt en dat heeft nadelige gevolgen voor onze economie. De regering toont echter weinig urgentie. Dat moet anders.
    - De regering kan ten eerste de zgn. “**Motie Franken**” als belangrijkste toets bij het ontwikkelen van beleid dat de privacy inperkt omarmen. Deze motie is aangenomen in de Eerste Kamer en de regering heeft de motie omarmd in het kader van cybersecurity. Nu moet de regering de motie toepassen bij algemeen beleid dat inbreuk maakt op de privacy.
    - Ten tweede zou de regering zo snel mogelijk een **meldplicht datalekken** moeten invoeren. Zij heeft dit al jaren geleden toegezegd en heeft dat zelfs in het regeerakkoord aangekondigd. Het wordt tijd dat de regering op zeer korte termijn een wetsvoorstel hiertoe naar de Tweede Kamer stuurt.
    - Ten derde zou de regering de **handhavingsmogelijkheden** van het College bescherming persoonsgegevens (“**Cbp**”) moeten versterken. De boetebevoegdheid van het CBP moet vergelijkbaar worden met de boetebevoegdheid in de Mededingingswet en de Telecommunicatiewet. Bovendien moet de bevoegdheid in ieder geval worden uitgebreid naar het recht op inzage, correctie en verwijdering.
    - Ten vierde zou de regering zich actief moeten mengen in het formuleren van **Europees en internationaal beleid** om de privacy van Nederlanders te beschermen.
    - Tot slot zou de regering het **meldingsregister en de meldingsplicht** moeten handhaven.

Privacybescherming wordt steeds belangrijker, maar regering toont weinig urgentie

2. Privacybescherming neemt een steeds belangrijkere rol in onze maatschappij in. Er gaat geen week voorbij of privacy haalt het nieuws. Van het meeluisteren naar internetverkeer door KPN, naar het doorverkopen van locatiegegevens door TomTom, tot het doorverkopen van privé-gegevens door apps voor smartphones. En steeds als bedrijven en organisaties inbreuk maken op de privacy van Nederlanders, neemt het vertrouwen van die gebruikers in online diensten af. Dit heeft tot gevolg dat men minder snel gebruik zal maken van die online diensten en dat is weer nadelig voor de online economie. Een goede bescherming van de privacy van alle Nederlanders is dan ook essentieel, niet alleen om principiële maar ook om economische redenen.

3. De regering zou hierin het voortouw moeten nemen. Iedere Nederlander wordt dagelijks geconfronteerd met privacy-inbreuken, maar de regering laat hier nog weinig daadkracht zien. De regering zou ambitieuzer moeten zijn en sneller beleid moeten formuleren. In het algemeen zouden we het parlement dan ook willen oproepen om de regering aan te sporen om de bescherming van de privacy serieuzer te nemen. Om een voorbeeld te geven: de regering kondigt al jaren aan dat zij een meldplicht datalekken zal introduceren, maar heeft nog steeds geen concreet wetsvoorstel geïntroduceerd.

De regering moet de toepassing van de Motie Franken bij privacy-inperkend beleid omarmen

4. Een van de makkelijkste en beste manieren om het beleid op het gebied van privacy in één klap te verbeteren, is door de zgn. “Motie Franken” te omarmen. De Eerste Kamer heeft begin dit jaar met grote meerderheid deze motie over de toetsing van privacybeperkende maatregelen aangenomen (**bijlage 1**).[1] De motie somt vijf criteria op waaraan nieuwe privacybeperkende maatregelen voorafgaand aan hun introductie getoetst moeten worden. De regering dient tevens verslag te doen van deze toetsing in de Memorie van Toelichting. De Tweede Kamer heeft deze motie vervolgens in het kader van de bespreking van de strategie op het gebied van cybersecurity overgenomen. Minister Opstelten heeft tijdens het debat zelfs toegezegd dat de Motie Franken inderdaad de leidraad wordt bij nieuwe wetgeving op het gebied van cybersecurity.[2]

5. De vijf criteria en de rapportage in de Memorie van Toelichting garanderen een gedegen besluitvorming op dit nieuwe en complexe onderwerp. Bovendien geeft dit kader het parlement direct inzicht in de beweegredenen van de regering om te pleiten voor het inperken van de privacy van Nederlanders. Bits of Freedom pleit er daarom voor dat het parlement tijdens het debat eist dat de regering ook in breder verband dan alleen cybersecurity de Motie Franken omarmt. De regering heeft hiervoor al een klein aanknopingspunt geboden, door in de privacynotitie te schrijven dat “wettelijke maatregelen op nationaal niveau behoren te zijn voorzien van een transparante toets aan de grondrechten”.[3]

> **Aanbeveling: Het parlement moet er bij de regering op aandringen dat zij tijdens het debat toezegt dat de criteria van de Motie Franken worden toegepast bij het ontwikkelen van beleid dat de privacy inperkt.**

1 Kamerstukken I 2011/12, 31 051, D.
2 Zie https://www.bof.nl/2011/06/03/kamer-stelt-grondrechten-centraal-in-cybersecuritybeleid/
3 Notitie privacybeleid, p. 11.

Meldplicht datalekken moet zo snel mogelijk worden ingevoerd

6. Bits of Freedom houdt sinds anderhalf jaar een Zwartboek datalekken bij, met de belangrijkste Nederlandse datalekken. Bijna iedere week wordt een datalek toegevoegd aan het zwartboek. Een voorbeeld van zo'n lek is het lek bij Kasboek, waar meer dan een miljoen banktransacties werden gelekt, met een totale waarde van EUR 200 miljoen en gemiddelde waarde van EUR 640 per transactie. Een groot deel van de transacties bevatten idenitificeerbare informatie, waaronder NAW- en rekeninggegevens. Een ander voorbeeld is de receptensite Smulweb, waar ongeveer één miljoen gebruikersgegevens, inclusief onversleutelde passwords buit zijn gemaakt door digitale inbrekers.

7. In het regeerakkoord is toegezegd dat zo een meldplicht zal worden geïntroduceerd. Het is nu tijd om de daad bij het woord te voegen. Het is belangrijk om zo snel mogelijk een meldplicht te introduceren. Pas als gebruikers worden geïnformeerd, kunnen zij immers maatregelen nemen om schade te voorkomen, zoals hun rekeningen extra goed gaan monitoren en hun passwords aanpassen. En bedrijven zullen een inbraak vaak maar al te graag geheim willen houden. De recente poging van certificaatverstrekker Diginotar om de inbraak in haar netwerk geheim te houden onderstreept dat: hierdoor is de vertrouwelijke communicatie van honderdduizenden Iraniërs in gevaar gebracht. In **bijlage 2** hebben wij een concreet voorstel voor zo een meldplicht uitgewerkt.

> **Aanbeveling: Het parlement moet bij de regering erop aandringen dat zij zo snel mogelijk een meldplicht datalekken introduceert, zodat gebruikers direct geïnformeerd worden als hun persoonsgegevens op straat zijn komen te liggen.**

Versterk de handhavingsmogelijkheden van het College bescherming persoonsgegevens

8. Naarmate steeds meer bedrijven en organisaties persoonsgegevens verwerken, zal het aantal overtredingen van de Wet bescherming persoonsgegevens ook toenemen. Het Cbp handhaaft de Wet bescherming persoonsgegevens (“**Wbp**”), maar heeft op dit moment slechts een beperkt handhavingsinstrumentarium. Zij kan geen hoge boetes opleggen, en bovendien maar voor een beperkt aantal overtredingen.

9. Het is daarom essentieel dat de handhavingsbevoegdheden van het Cbp worden versterkt, zodat zij stevige boetes kan opleggen voor privacy-overtredingen. De boetebevoegdheid van het Cbp zou, net zoals dat het geval is bij overtredingen van de Mededingingswet en de Telecommunicatiewet, maximaal EUR 450.000 of, als dat meer is, 10% van de jaaromzet van onderneming in Nederland moeten zijn bij zware overtredingen. Bovendien zou de handhavingsbevoegdheid zich onder moeten uitstrekken tot het recht op inzage, correctie en verwijdering (art. 35 Wbp): juist met dat recht kan iedere Nederlander immers inzicht krijgen in de enorme hoeveelheid gegevens die over hem of haar verzameld wordt.

> **Aanbeveling: Het parlement moet er bij de regering op aandringen dat zo snel als mogelijk de handhavingsbevoegdheden van het Cbp worden gelijkgetrokken met die van de NMa en de OPTA, en zich ook uitstrekken tot overtredingen van het recht op inzage en verwijdering.**

Neem actief deel aan het vormen van Europees en internationaal privacybeleid

10. De bescherming van de privacy is niet een puur nationale aangelegenheid: de gegevens van Nederlandse burgers worden steeds meer opgeslagen op servers van buitenlandse bedrijven, zoals Google, Amazon en Microsoft. Nederlanders hebben weinig zicht op wat precies met die gegevens gebeurt, laat staan dat ze daar veel invloed op kunnen uitoefenen. Dat zou anders moeten: de regering zou zich hard moeten maken in Europees en internationaal verband om te zorgen dat de privacy van Nederlanders beschermt blijft, ook als zij gebruik maken van online diensten van buitenlandse bedrijven.

> **Aanbeveling: Het parlement moet er bij de regering op aandringen dat zij zich actief mengt bij het formuleren van Europees- en internationaal beleid om de privacy van Nederlandse burgers te beschermen.**

Handhaaf het meldingsregister en de meldingsplicht

11. Bits of Freedom heeft een website waarmee Nederlanders het recht op inzage bij bedrijven en organisaties kunnen effectueren. Op deze website kan een gebruiker aangeven welke bedrijven en organisaties hij graag zou willen aanschrijven, en vervolgens worden automatisch brieven gegenereerd. De databank met bedrijvenen organisaties die gegevens verzamelen, kan samengesteld worden aan de hand van het meldingsregister van het Cbp (waarin iedere verwerker van persoonsgegevens verplicht moet melden dat hij persoonsgegevens verwerkt). Het is dus belangrijk dat dit meldingregister intact blijft.

> **Aanbeveling: Het parlement moet er bij de regering op aandringen dat de meldingsplicht van bedrijven en organisaties bij het Cbp gehandhaafd blijft.**

Tot slot

12. Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd. Mocht u nog vragen hebben naar aanleiding van deze notitie, aarzel dan niet om contact met mij op te nemen. Mijn contactgegevens staan boven aan deze brief.

Hoogachtend,

Ot van Daalen

BIJLAGE 1

Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2010–2011

31 051 Evaluatie Wet bescherming persoonsgegevens

D

MOTIE VAN HET LID FRANKEN C.S.
Voorgesteld 17 mei 2011

De Kamer,

gehoord de beraadslaging,

overwegende, dat het grondrecht op bescherming van de persoonlijke levenssfeer in onze democratische rechtsstaat van groot belang is,

overwegende, dat er tendensen zijn om bij nieuwe wetgeving de mogelijke beperkingen op dit grondrecht uit te breiden en te versterken,

overwegende voorts, dat bij het totstandbrengen van nieuwe wetgeving uitdrukkelijk aandacht moet worden gegeven aan de vraag of de beperkingen op het grondrecht tot bescherming van de persoonlijke levenssfeer gerechtvaardigd zijn,

overwegende, dat voor de beantwoording van deze vraag aansluitend aan de verdragsverplichting moet worden getoetst aan de volgende criteria:
1. De noodzaak, effectiviteit en hanteerbaarheid van de maatregel,
2. De proportionaliteit: de inbreuk mag niet groter zijn dan strikt noodzakelijk is,
3. De resultaten van een Privacy Impact Assessment, zodat vooraf is onderzocht welke risico's de maatregel met zich meebrengt,
4. De mogelijkheid van een effectief toezicht en controle op de uitvoering van de maatregel, te realiseren door onder meer audits door de onafhankelijke toezichthouder,
5. Beperking van de geldigheidsduur door een horizonbepaling of in ieder geval een evaluatiebepaling,

verzoekt de regering bij wetsvoorstellen, waarbij van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer sprake is, de hierboven genoemde criteria in de afweging en besluitvorming te betrekken en daarvan in de memorie van toelichting bij het betreffende wetsvoorstel verslag te doen,

en gaat over tot de orde van de dag.

kst-31051-D
ISSN 0921 - 7371
's-Gravenhage 2011

Franken
Tan
Strik
Holdijk
Slagter-Roukema
Staal

BIJLAGE 2

BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

Position Paper

Meldplicht datalekken

25 januari 2010

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Position Paper
Meldplicht datalekken

25 januari 2010

Over dit stuk

Bits of Freedom verdedigt communicatievrijheid en privacy in de informatiemaatschappij. Dit paper is geschreven door Bits of Freedom met medewerking van Koen Versmissen en anderen. Alleen Bits of Freedom is verantwoordelijk voor de inhoud en de eindredactie van dit paper.

Contact

Ot van Daalen
+31(0)654386680
ot.vandaalen@bof.nl

1. SAMENVATTING

1. Onze persoonsgegevens komen in steeds meer databanken voor. Die databanken zijn, mede doordat ze steeds vaker met internet verbonden zijn en doordat op een drager steeds meer gegevens kunnen worden opgeslagen, steeds moeilijker goed te beveiligen.

2. De kans op datalekken (het in verkeerde handen vallen van persoonsgegevens als gevolg van verlies of diefstal) neemt daardoor toe. Datalekken kunnen tegelijkertijd vergaande consequenties hebben voor betrokkenen: identiteitsfraude, ongewenste profilering, de-anonimisering en direct-marketing. Bovendien is verlies van vertrouwen in ICT een serieus risico van datalekken.

3. Om betrokkenen in staat te stellen hun schade te beperken zou de Nederlandse overheid volgens Bits of Freedom een verplichting om datalekken te melden moeten introduceren: een “meldplicht datalekken”. Die meldplicht zou moeten gelden voor alle verwerkingen waarop betrokkenen een inzage- en correctierecht hebben, dus zou zowel voor bedrijfsleven, NGO's als de overheid moeten gelden. Datalekken zouden gemeld moeten worden aan (potentiële) slachtoffers en het College Bescherming Persoonsgegevens (“**CBP**”). Zowel vastgestelde als vermoede datalekken zouden onder de meldplicht vallen. De beperkte meldplicht zoals voorgeschreven in de ePrivacy-richtlijn is onvoldoende: het kabinet zou de herziening van de Wet bescherming Persoonsgegevens (“**Wbp**”) moeten aangrijpen om een brede meldplicht op te nemen.

4. Dat wordt hieronder toegelicht.

2. MEER PERSOONSGEGEVENS WORDEN OPGESLAGEN IN DATABANKEN

5. Meer en meer van onze persoonsgegevens vinden massaal hun weg naar grote databanken. Niet alleen omdat het steeds gemakkelijker en goedkoper wordt om persoonsgegevens elektronisch op te slaan, maar vooral ook doordat een steeds groter deel van ons leven zich online afspeelt. Met iedere stap die we online zetten laten we een digitaal spoor achter. Die gegevens kunnen eenvoudig worden opgeslagen en in theorie voor altijd met ons geassocieerd worden. In een onderzoek in opdracht van het CBP wordt geschat dat gegevens over de gemiddelde Nederlander in tussen de 250 en duizenden databanken zijn geregistreerd.[1]

6. In het kader van verschillende projecten van de overheid worden uitgebreide gegevens over burgers opgeslagen. Telecomgegevens worden opgeslagen en toegankelijk gemaakt in het kader van de Wet bewaarplicht telecommunicatiegegevens. Reisdocumenten worden van biometrie voorzien, en deze biometrische kenmerken worden opgeslagen in databanken. Grote hoeveelheden privacygevoelige gegevens komen straks terecht in ons digitaal klantdossier in de sociale zekerheid, in ons elektronisch patiëntendossier en in het elektronisch kinddossier van onze kinderen. Dankzij de OV-chipkaart en straks de kilometerheffing (afhankelijk van de implementatie) zal ons reisgedrag tot in detail worden

1 Zie voor meer informatie over deze thematiek bijvoorbeeld Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (New York University Press, 2004) en Bart Schermer & Ton Wagemans, Onze digitale schaduw: Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat (Considerati, 2009).

geregistreerd en bewaard. Die bestanden worden vervolgens in toenemende mate aan elkaar gekoppeld.

7. Daarnaast legt de private sector grote databanken met informatie over hun klanten aan. Dat kunnen gegevens zijn die van de klant zelf verkregen zijn, maar het kan ook gaan om gegevens die van derden zijn verkregen (al of niet in strijd met de wet). Banken en winkels beschikken over uitgebreide databanken met de transacties van al hun klanten. Dienstverleners houden precies bij hoe hun klanten gebruik maken van hun dienst. Ook niet-commerciële instellingen houden grote databanken bij, bijvoorbeeld met adressen van donateurs.

3. DE KANS OP DATALEKKEN NEEMT TEGELIJKERTIJD TOE

8. Naarmate er meer en meer persoonsgegevens worden opgeslagen in steeds meer databanken, neemt ook de kans dat deze gegevens in verkeerde handen komen toe: “hoe meer je opslaat, hoe meer je kan kwijtraken”. Er zijn daarnaast twee factoren die deze ontwikkeling versterken. In de eerste plaats maken organisaties databanken vaak (voor intern gebruik) toegankelijk via het internet. Het goed beveiligen van een databank is op zich al ingewikkeld, en als deze databanken aan het internet worden verbonden wordt dit extra moeilijk doordat deze voor meer mensen zichtbaar en toegankelijk worden. De kans op een inbraak of toevallige ontsluiting van data via internet neemt daarmee toe. Ten tweede passen er steeds meer gegevens op eenvoudig te vervoeren gegevensdragers zoals CD/DVD-ROMs en USB sticks. Geregeld worden er grote hoeveelheden gegevens uit databanken slecht of in het geheel niet beveiligd op zo’n mobiele gegevensdrager gezet, en het risico van misbruik bij verlies of diefstal wordt daarmee erg groot.

9. Ter illustratie worden hieronder een aantal in het oog springende casussen uit 2009 in Nederland gememoreerd:

- In december 2009 is een USB-stick met de gegevens van 3.000 klanten van de Rabobank kwijtgeraakt. De stick bevatte persoonsgegevens, beleggingsvormen en in veel gevallen de hoogte van het belegde vermogen.[2]
- Het adresboek van persbureau GPD bleek in augustus 2009 voor iedereen via Google beschikbaar te zijn gemaakt. Hierdoor zijn de telefoonnummers van bekende Nederlanders die een geheim nummer hebben, waaronder Geert Wilders en Gerard Spong, beschikbaar gekomen.
- Het Dagblad van het Noorden heeft in mei 2009 meer dan 32.000 emailadressen van haar klanten per ongeluk toegankelijk gemaakt via haar website.[3] De adressen zijn geïndexeerd in zoekmachines.
- Door een fout in de website van de Geschillencommissie waren alle lopende en afgesloten dossiers tot 2005 online in te zien door personen die een geschil hadden lopen.[4] Dit zijn tienduizenden geschillen. De dossiers bevatten gevoelige persoonsgegevens, zoals jaarafrekeningen, bankafschriften en NAW-gegevens. Pas in april 2009 is dit lek ontdekt door een journalist en de website is vervolgens off-line

2 Zie http://www.gelderlander.nl/voorpagina/5961111/Bankgegevens-op-straat.ece.
3 Zie http://weblog.fok.nl/viewSingleItem/25294/Bedankt-Dagblad-vh-Noorden!.htm.
4 Zie http://nos.nl/artikel/85135-lek-in-beveiliging-geschillencommissie.html.

gegaan.

- Een site waar gratis condooms konden worden besteld, maakte de gegevens van al haar klanten – ongeveer 10.000 – per ongeluk on-line beschikbaar. De site was juist bedoeld voor personen die zich schaamden om via een winkel condooms te kopen. Dit lek kwam in februari 2009 aan het licht.[5]

10. Ook in andere landen is dit een groot probleem: in de Verenigde Staten zijn bijvoorbeeld 316 incidenten geregistreerd in de "data loss database". In totaal ging het om de gegevens van meer dan honderd miljoen personen. Het werkelijke aantal ligt waarschijnlijk veel hoger, aangezien bij veel incidenten onbekend is hoeveel gegevens zijn uitgelekt of gevaar liepen. Er zijn honderden vergelijkbare verhalen in andere landen. In het Verenigd Koninkrijk zijn in 2007 CD-rooms met de bankgegevens van 25 miljoen Engelsen (iedereen die recht heeft op kinderbijslag) kwijtgeraakt.[6]

4. DATALEKKEN KUNNEN GROOT PROBLEEM ZIJN VOOR BETROKKENEN

11. Datalekken brengen diverse risico's met zich, doordat de weggelekte gegevens op verschillende manieren oneigenlijk gebruikt kunnen worden.

- Het belangrijkste risico van grote hoeveelheden gegevens die weglekken is identiteitsfraude. Persoonsgegevens zijn goud waard voor criminelen, die hiermee andermans identiteit aan kunnen nemen en zo fraude kunnen plegen. Identiteitsfraude is vaak een wat "onzichtbaar" fenomeen, aangezien vooral aandacht bestaat voor de misdrijven die volgen op identiteitsfraude, zoals het leeghalen van bankrekeningen. In de Verenigde Staten wordt identiteitsfraude niettemin al jarenlang erkend als een serieus probleem. In 2006 zijn meer dan 8 miljoen Amerikanen het slachtoffer geworden van identiteitsfraude. Ook in Nederland mag dit probleem zich langzamerhand verheugen in verhoogde aandacht, mede als gevolg van de grote media-aandacht voor de zaak van Ron Kowsoleea, die vijftien jaar lang last heeft gehad van het feit dat hij slachtoffer is van identiteitsfraude. Bij het Meldpunt Identiteitsfraude zijn in nog geen jaar tijd honderden meldingen van identiteitsfraude ontvangen. Dit lijkt erop te wijzen dat identiteitsfraude ook in Nederland een probleem van serieuze omvang is of aan het worden is.
- Een tweede risico van deze datalekken is dat gebruikers met verkregen gegevens van bepaalde diensten kunnen worden uitgesloten, of op een andere manier nadelig behandeld kunnen worden. Zo kan je een verzekering geweigerd worden als door een lek bekend wordt dat je tot een risicogroep behoort. Omdat dit soort uitsluiting niet altijd wenselijk is, heeft de wetgever grenzen gesteld aan de persoonsgegevens die met het oog op dit soort selectie verwerkt mogen worden. Als gevolg van datalekken kunnen deze gegevens echter in sommige gevallen toch hun weg vinden naar plekken waar ze niet thuishoren. Het is goed voorstelbaar dat er handelsinformatiebureau's zijn die hiermee hun geld verdienen.
- Een derde risico van deze datalekken, is dat de bewust gekozen anonimiteit van gebruikers hierdoor kan worden opgeheven. Gebruikers die hun identiteit slechts wilden delen met specifieke dienstverleners, zien gevoelige gegevens op straat liggen. Ook

5 Zie http://www.nu.nl/internet/1914254/fout-onthult-klantendatabase-condoomgebruikers.html
6 Zie http://news.bbc.co.uk/2/hi/7103566.stm.

kunnen gegevens die worden gelekt, soms in combinatie met reeds beschikbare gegevens leiden tot opheffing van anonimiteit: zo kon aan de hand van geanonimiseerde gebruikersinformatie die door een videoverhuurbedrijf op internet beschikbaar was gesteld, een vrouw toch geïdentificeerd worden (en ook haar seksuele geaardheid kon worden achterhaald).[7]

- Een vierde risico van deze datalekken, is het verlies van vertrouwen in ICT, waaronder e-commerce en e-banking. Gebruikers zullen steeds terughoudender zijn met het vertrouwen van hun gegevens aan dienstverleners, als zij niet weten wat vervolgens met die gegevens gebeurt, en als zij niet op de hoogte worden gesteld als het misgaat. Hierdoor zullen diensten die slechts verstrekt kunnen worden met behulp van deze gegevens, minder goed functioneren.
- Tot slot is het risico dat deze gegevens gebruikt worden om mensen ongevraagd te benaderen. Dat is vaak in strijd met wet- en regelgeving, maar dat weerhoudt bedrijven er vaak niet van om mensen te benaderen. Spam is hiervan een goed voorbeeld.

5. BETROKKENEN MOETEN WORDEN GEINFORMEERD OVER DATALEKKEN

12. Organisaties hebben er bij datalekken lang niet altijd belang bij om de slachtoffers daarvan op de hoogte te stellen. Niet alleen is het kwaad waar het de organisatie in kwestie betreft immers al geschied, ook kan deze in een ongunstig daglicht komen te staan wanneer breed bekend wordt dat er een datalek heeft plaatsgevonden. In de praktijk zijn er ook voorbeelden bekend van datalekken die (aanvankelijk) voor de slachtoffers verborgen werden gehouden.

13. Het is tegelijkertijd belangrijk dat slachtoffers snel op de hoogte worden gebracht van het feit dat persoonsgegevens van hen gecompromitteerd, of mogelijk gecompromitteerd zijn. Het tijdig en volledig informeren van slachtoffers van datalekken kan identiteitsfraude weliswaar niet geheel voorkomen, maar kan de slachtoffers wel in staat stellen om schadebeperkende maatregelen te nemen, zoals het laten blokkeren van hun credit card. En waar het niet mogelijk is om dit soort maatregelen te nemen, zal het informeren van de slachtoffers in ieder geval leiden tot verhoogde waakzaamheid, zodat bij het eerste teken van identiteitsfraude alsnog kan worden ingegrepen. De andere genoemde risico's van datalekken zullen in het algemeen minder gemakkelijk te voorkomen zijn door een slachtoffer dat op de hoogte is gebracht. Niettemin geldt ook daar dat bekendheid met het datalek tot verhoogde alertheid zal leiden, en daardoor zal helpen bij het blootleggen van het oneigenlijke gebruik van informatie.

14. Ook is het van belang dat organisaties meer open moeten zijn over datalekken. Indien zij niet alleen de slachtoffers moeten informeren, maar ook het algemene publiek, dan heeft dat verschillende positieve effecten:

    - Door bekendheid met de soort en hoeveelheid datalekken die voorkomen zullen burgers zich beter bewust worden van de gevaren van de opslag van hun gegevens in grote databanken, zeker als die slecht beveiligd worden. Dit stelt ze in staat om zich kritischer op te stellen jegens de beheerders van die databanken.

7 Zie http://www.volkskrant.nl/binnenland/article1329274.ece/Lesbische_moeder_daagt_online_videotheek_voor_de_rechter.

- Organisaties zullen uit angst voor reputatieschade hogere prioriteit geven aan goede beveiliging van de persoonsgegevens die zij beheren, opdat zij datalekken zoveel mogelijk kunnen voorkomen.
- Ministeries, toezichthouders, brancheorganisaties en anderen zullen zo kunnen beschikken over actuele en volledige beleidsinformatie over datalekken.

15. Het is dan ook niet verbazingwekkend dat in verschillende landen en in Nederland de roep om een meldplicht datalekken toeneemt. De meldplicht datalekken is al in meerdere landen geïntroduceerd, waaronder onlangs in Duitsland (zie onder meer het rapport “Melding Maken” van Research voor Beleid, gepubliceerd op 17 april 2009, voor een deeloverzicht hiervan). Op Europees niveau wordt deze meldplicht datalekken in het kader van de herziening van de ePrivacy-richtlijn (2002/58/EG) ingevoerd, maar die geldt slechts voor de telecommunicatiesector. Bovendien pleit de Artikel 29-werkgroep voor een vergelijkbare meldplicht (zie opinie 1/2009 van 10 februari 2009). Peter Hustinx van de Europese toezichthouder voor persoonsgegevens heeft in 2008 opgeroepen tot een bredere meldplicht voor datalekken.[8] Officier van justitie Speijers, CBP-voorzitter Kohnstamm en D66-leider Pechtold hebben in 2008 ook opgeroepen tot een wettelijke meldplicht bij diefstal van persoonsgegevens van klanten.[9] Ook de PvdA wil een meldplicht instellen voor grote bedrijven na inbraak in hun computersystemen.[10]

16. Hoewel reeds een beperkte meldplicht voor telecomaanbieders in de ePrivacy-richtlijn is opgenomen, is de door Bits of Freedom voorgestelde meldplicht breder: deze ziet op alle soorten databanken. Er is in de media te lezen dat op Europees niveau een bredere meldplicht in de maak is. Het duurt echter te lang om daarop te wachten: Nederland kan de implementatie van de herziening van de ePrivacy richtlijn aangrijpen om een brede meldplicht op te nemen. Dat zou passen in het beleid zoals aangekondigd in de brief van de Minister van Binnenlandse Zaken van 8 april 2009 aan de Tweede Kamer, waarin wordt aangekondigd dat het kabinet “na afronding van de besluitvorming op Europees niveau [zal] overgaan tot nationale implementatie en een meldplicht [zal] invoeren in geval van verlies van persoonsgegevens uit datasystemen”. Daarbij zal gebruik worden gemaakt van de kennis die is opgedaan uit het rapport “Melding maken?'. Daarom zou het kabinet reeds nu een meldplicht datalekken volgens de volgende richtlijnen moeten introduceren.

A.1 Wie moet melden?

Zoals we hebben gezien ontstaan er op steeds meer plaatsen grote databanken: zowel in de publieke als de private sector. Bits of Freedom vindt dan ook dat de meldplicht datalekken voor alle organisaties moet gelden. Of, in termen van de Wet bescherming persoonsgegevens: een meldplicht datalekken geldt voor alle verantwoordelijken.

A.2 Bij wie moet er gemeld worden?

(Mogelijke) datalekken moeten in beginsel worden gemeld bij zowel de (mogelijke) slachtoffers als bij een onafhankelijk overheidsorgaan. Gelet op de noodzakelijke breedte van de meldplicht en het feit dat het om, vaak gevoelige, persoonsgegevens gaat, vindt Bits of Freedom dat het bijhouden van meldingen het beste bij het College Bescherming

8 Zie http://webwereld.nl/nieuws/50725/eu-waakhond-pleit-voor-meldplicht-informatielekken.html.

9 Zie http://webwereld.nl/nieuws/53492/roep-om-meldplicht-datalekken-zwelt-aan.html.

10 Zie http://webwereld.nl/nieuws/50548/pvda-wil-meldplicht-computercriminaliteit.html.

Persoonsgegevens kan worden neergelegd.

A.3 Wat voor soort datalekken moeten gemeld worden?

Bits of Freedom vindt dat zowel vastgestelde datalekken als vermoede datalekken moeten worden gemeld. Met vermoede datalekken bedoelen we beveiligingsinbreuken waarvan niet duidelijk is of als gevolg daarvan ook persoonsgegevens in verkeerde handen terecht zijn gekomen. Verder doet het er in de ogen van Bits of Freedom niet toe hoeveel of wat voor gegevens er zijn ontvreemd: alle datalekken zouden meldingsplichtig moeten zijn.

A.4 Tekstvoorstel wijziging Wbp

Aan de Wet bescherming persoonsgegevens (Wbp) wordt een artikel 13a toegevoegd, dat als volgt luidt:

1. De verantwoordelijke die weet, of redelijkerwijs kan vermoeden, dat onbevoegd toegang is verkregen tot door hem verwerkte persoonsgegevens, stelt de betrokkenen daarvan onverwijld op de hoogte.
2. De verantwoordelijke als bedoeld in het eerste lid stelt eveneens het College onverwijld op de hoogte.
3. Het College houdt een openbaar register bij van de meldingen die het ontvangt uit hoofde van het tweede lid.
4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wijze waarop de meldingen dienen te geschieden.

Aan de lijst van artikelen in artikel 15 Wbp wordt het nieuwe artikel 13a toegevoegd. In de toelichting dient duidelijk gemaakt te worden dat de zinsnede “redelijkerwijs kan vermoeden” ook van toepassing is op beveiligingsinbreuken waarvan niet bekend is of die tot onbevoegde toegang tot gegevens hebben geleid. Met “onbevoegde toegang” wordt gedoeld op toegang die is verkregen in strijd met technische beveiligingsmaatregelen of juridische waarborgen. De verantwoordelijk moet de betrokkenene op de hoogte stellen van de specifieke persoonsgegevens waartoe mogelijk onbevoegd toegang is verkregen. Het is dus niet voldoende om alleen te melden *dat* onbevoegd toegang is gekregen.

Daarnaast zou de Nederlandse overheid bedrijven en organisaties moeten ondersteunen bij de stappen die ze moeten nemen als sprake is van een datalek. In de Verenigde Staten bestaat al veel ervaring met “data breaches”. De Federal Trade Commission biedt actieve ondersteuning aan bedrijven en organisaties die betrokken zijn bij een datalek, onder meer door voorlichting via haar website.[11] De gedachte hierachter is dat een meldplicht niet alleen een sanctie is voor slechte beveiliging, maar dat het ook bedoeld is om verdere schade te voorkomen. Bedrijven en organisaties die geholpen worden met het snel informeren van slachtoffers, zullen zo meer schade kunnen voorkomen.

11 Zie http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html.