SİZİ KİM GÖZETLİYOR?

Bazılarının "akvaryum toplumu" diye adlandırdıkları, belli teknolojilerin kullanılması yoluyla sürekli izlenen ve gözetlenen toplumu yaratan teknolojiler aslında yeni değil. Yeni olan, bu teknolojilerin her an, her yerde bulunuyor olmaları. Bu durumun en iyi örneklerinden biri, ABD ordusu tarafından 1960 yılında tasarlanan GPS teknolojisinin, aradan 20 yıl geçtikten sonra her yerde kullanılır hale gelmiş olması ve bu teknolojiye ait endüstrinin öngörülen 2008 yılı bütçesinin de 28 milyar dolar olması. Milyonlarca arabaya GPS teknolojisi yerleştiren sistemler yoluyla, sivil halk tarafından kullanılan tüm arabalar polis ve devlet kurumlarının istekleri doğrultusunda izlenebiliyor.

GPS teknolojisinin cep telefonlarında kullanılmaya başlanmasıysa yeni tartışmaları gündeme getirdi. ABD'deki federal düzenlemeler tüm cep telefonu ağlarının E911 adı verilen bir sistemle donatılmış olmasını gerektiriyor. Bu sistem, üç cep telefonu kulesinin arasında kalan bölgeyi üçgenlere ayırarak bir cep telefonunun konumunu 100 metre yakınına kadar, GPS teknolojisini kullandığındaysa yaklaşık 40 santimetre yakınına kadar bulabiliyor. E911, birileri polis imdat, hızır acil servis gibi acil yardım servislerini aradığında konum bilgisini gönderiyor gibi görünse de, konum tabanlı servisleri birleştirmiş olan daha yeni model telefonlarda, kesin konum bilgisi cep telefonu operatörüne sürekli olarak geri gönderiliyor. Bu da her bir yeni cep telefonunun aslında yeni bir cep dinleme cihazı olması anlamına geliyor.

450 dolarlık aşırı hız cezası alan bu adamın cezası, polis tarafından değil, arabalarına GPS cihazı yerleştiren araba kiralama firması tarafından verilmişti.

E911 teknolojisi kamu yararına bir servişmiş gibi tasarlanmışsa da, bazılarına göre kötüye kullanma amacına hizmet eden bir bekçi köpeği. Bu teknoloji nedeniyle yaşanan bazı olaylar, şimdiden mahkeme yolunu tutmuş bile. ABD'de 2004 yılının Ağustos ayında Ara Gabrielyan isimli bir vatandaş, ne yaptığını izlemek için eski kız arkadaşının arabasına, kayıt yapabilen GPS özellikli bir telefonu gizlice yerleştirmek suçundan tutuklanmış. Bazıları bu tür girişimleri "21. yüzyılın avcılığı" olarak adlandırıyor. Şimdilerde gizlice izlemek ve terör tehditlerinde bulunmak suçlarıyla mahkemeye çıkarılan ve 500.000 dolar kefaletle mahkeme gününü beklemek üzere serbest bırakılan Gabrielyan, cep telefonu sahiplerinin, telefonlarını İnternet üzerinden izlemelerini sağlayan yeni servislerden birine ait bir sözleşmeyi imzalamış. ABD'deki belli İnternet siteleri yoluyla, bir cep telefonunun konumu ve hangi hızla hareket ettiği, tümü caddeler düzeyinde ayrıntılandırılmış dijital haritalar üzerinde izlenebiliyor. Çok sayıda eleştirinin hedefi olan bu "ken-

Dijital Hapishane

Yaşamlarımızı daha güvenli, daha basit ve daha hızlı hale getiren teknolojinin bize sağladığı her bir kolaylık, aslında izlenmemizi kolaylaştıran yeni bir ipucu anlamına geliyor. Bu teknolojileri kullanma düzeyimiz arttıkça arabamızda, bilgisayarımızda, süpermarkette ve hatta yolda yürürken bile arkamızda başkaları tarafından izlenebilecek izler bırakır hale geliyoruz. Bu konuda dikkatli olmak ve bu teknoloji yoluyla kendimizle ilgili olarak yaydığımız verileri kimlerin, ne amaçla topladığı konusunda duyarlı olmak gerekiyorsa da, en azından şimdilik bir kulübe alıp ormana yerleşerek herşeyden uzak bir yaşam sürmemize gerek yok. Hem bu teknolojilerin nimetlerinden yararlanıp, hem de özel hayatımınızın gizliliğini sağlamak için bazı şeylere dikkat etmeniz yeterli. İşte özel hayatınızın gizliliğini sağlamanız için size bazı ipuçları:

Alışverişte

- Büyük mağaza zincirlerinin hemen hemen tümünün sunduğu kulüp üyeliği, abonelik, sürekli müşteri kartı türündeki olanakları kullanmaktan kaçının. Çünkü bu tür bir kart, ödemeniz gereken tutarı azaltıyorken, diğer yandan da ne zaman ne satın aldığınızın sürekli olarak büyük bir veritabanında kaydedilmesini, böylece satın alma alışkanlıklarınızın belirlenmesini ve gerektiğinde başkaları tarafından kullanılabilmesini olanaklı kılıyor.
- Büyük süpermarketler yerine daha küçük marketlerden ve bakkallardan alışveriş yapmaya özen gösterin. Çünkü böyle mağazalar genellikle gelişkin veri toplama yöntemlerini kullanmıyorlar.
- Alışverişleriniz için kredi kartınız yerine bankamatik kartınızı kullanın. Bankamatik kartı kullanılarak yapılan para aktarımlarında yalnızca ödediğiniz ücretler kaydediliyor, alışverişinizdeki nesneler listelenmiyor.

Aşırı Evhamlılar İçin: Tüm banka, kredi ve alışveriş kartlarınızı alüminyum folyo ile kaplayın. Alüminyum folyo, radyo frekanslı tanıma sistemlerini durduruyor ve böylece süper bir koruyucu şapka görevi yapıyor.

Bilgisayarınızda

- Bilgisayarınıza mutlaka bir koruma duvarı yazılımı (firewall) ve casus kovucu (spyware) yazılımı yükleyin.
- Bu yazılımların her ikisini de sık sık güncelleyin.
- Kendinize çok karmaşık parolalar seçin. En iyi parolalar, bir kenara yazmadığınız sürece asla hatırlayamayacağınız kadar karmaşık olanlarıdır.
- IP adresinizi kapatın. Proxy sunucular kullanan bazı yazılımlar yoluyla İnternet'teki web sitelerinin, bilgisayarınızın kimliğini tanımalarını engelleyebilirsiniz.

Aşırı Evhamlılar İçin: Hiç risk almak istemiyorsanız, bilgisayar yerine daktilo kullanabilirsiniz. Zira henüz hiç bir daktiloya virüs bulaşmadı ve hiç bir daktilo korsan saldırısına uğramadı!!

Arabanızda

- Otomatik geçiş etiketlerinizi hiç açmadan satın aldığınız haliyle bir kenarda saklayın ve nakit ödeme sırasını kullanın. Biraz daha uzun süre kuyrukta beklemeniz gerekebilecek olsa da, böylece patronunuz ağır hasta olan yakın akrabanızın en yakındaki tatil kasabasında oturduğunu asla bilemeyecek!
- Araba kiralarken küçük harflerle yazılmış sözleşmeyi dikkatlice okuyun. Arabayı kiraladığınız şirket eğer arabaya GPS izleme sistemi yüklemişse ve buna bağlı olarak hız ya da belli bölge sınırlarını geçmekle ilgili bir uygulama yapıyorsa, bu durum burada yazacaktır.

Aşırı Evhamlılar İçin: Otobüse binerken bozuk paranızı ya da biletinizi hazırlamayı unutmayın.

Cep Telefonunuzda

- Telefonunuzun menü fonksiyonunu kullanarak konum tabanlı servislerin tümünü kapatın. Böylece telefonunuz yalnızca gerçekten acil servisleri aradığınızda operatörünüze bilgi iletecektir.
- Kontörlü hat kullanın. Bazı operatörlerde kontörlü bir hat alabilmek için yalnızca isminizi vermeniz yeterli olabiliyor ve bu ismin gerçekten size ait olup olmaması tamamen size kalmış. Bazılarıysa tümüyle gizlilik olanağı sağlayabiliyor.
- Kullanmadığınız zamanlarda telefonunuzu kapatın.

Aşırı Evhamlılar İçin

Evinizin ya da işyerinizin dışında sokakta yürürken telefonunuz çalarsa asla açmayın, birilerini aramanız gerekirse de aramayın. Kısaca dışarıda hiçbir telefon görüşmesi yapmayıp tüm görüşmelerinizi içerilerde yapmaya özen gösterin. GPS çipleri bina içlerinde bir tespit yapmakta güçlük yaşıyor.

din pişir, kendin ye" türünden izleme servislerini sunan İnternet sitelerinden bazılarının, "özel hayata saygı" gruplarınca en "istilacı" şirketler olarak etiketlenmiş olmalarına karşın, GPS yoluyla izlemeyi kazançlı bir işe çevirmeye çalışan girişimcilerin sayısında hiçbir azalma ya da geri çekilme yok. Üstelik bazı şirketler daha ileri düzeyde izleme olanakları yaratmak için bu teknolojilerin daha gelişkin kullanım yollarını bulmanın çabası içindeler. ABD'de bir şirket kablosuz iletişim, GPS izleme, dijital haritalama, yapay zeka ve İnternet gibi beş ayrı teknolojinin entegre edilmesi yoluyla çalışan "telematics" isimli bir sistemi geliştiriyor. Bazı araba kiralama şirketleri, büyük dağıtım şirketleri ve ticari tekne sahipleri tarafından kullanılan bu düşük maliyetli ileri teknoloji sistemini, çocuklarının aşırı hız yapmasını engellemek için talep edenler bile var. Çocuklarının arabalarına bu sistemden yerleştirmiş olan ebeveynlerin cep telefonlarına, çocukları belli bir hız sınırını aştığında bir dakikadan daha az bir sürede bir uyarı mesajı geliyor. Ebeveynler için oldukça yararlı ve iyi niyetli bir sistem gibi görünse de son kararı vermek için aslında bir de bu sistemi kullanan ailelerin çocuklarının ne düşündüklerini sormak gerek.

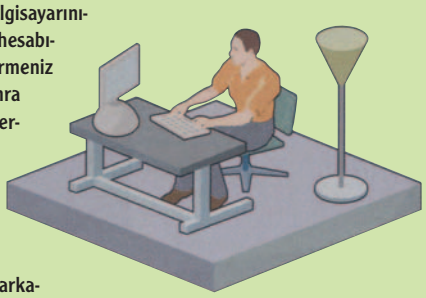
Bu çocukların ne düşündüklerini tam olarak bilemesek de, araba kiralama şirketi müşterilerinin bu sistemden nefret ettikleri ortada. Kiralık araç sektöründeki bilinen tüm büyük şirketler, bu tür teknolojileri yalnızca tüm bir filoyu izlemelerinin gerektiği durumlarda kullandıklarını söylüyorlar. Ama bu teknolojiyi başka amaçlara hizmet edecek biçimde kullanan bazı daha küçük şirketlere karşı 2004'te düzinelerce şikayet ve itiraz dilekçeleri yazıldı. Örneğin bu teknolojiyi, kiralama sözleşmesinde çok küçük harflerle yazılı olan "eyalet sınırını aşmama" kuralına uyulup uyulmadığını anlamak için kullanan bir şirket, 2003 yılında Kanadalı bir turisti, kendilerinden kiraladığı arabayla California eyaletinin dışında gittiği her bir kilometreye karşılık belli bir ücretle cezalandırmış. Bu durumda vermesi gereken araba kiralama ücreti bir anda 260 dolardan 3400 dolara fırlayan Kanadalı turistle şirket arasındaki tartışma hem mahkemeye, hem de tüm kamuoyuna yansımış. Neyse ki yasa yapıcılar, bu tür bir izlemenin gözardı edilemeyeceği konusunda hemfikir. California ve New York'ta, araba kiralama şirketlerinin aşırı hız ya da eyalet sınırını geçme gibi konularda ceza uygulamak amacıyla GPS teknolojisini kullanarak araçlarını izlemesini yasaklayan kurallar, şimdiden yasalaştırılmış durumda.

Çeviri:
Ayşenur Topçuoğlu Akman

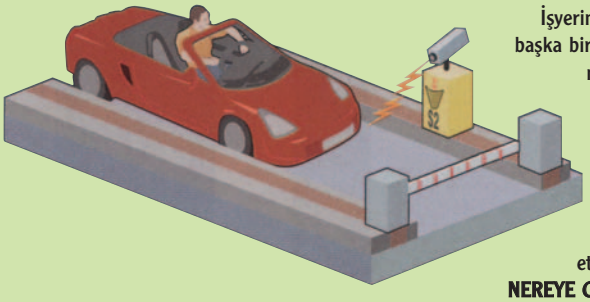
Kaynak: Cooper, S.; "Who's Spying On You?", Popular Mechanics, 23 Kasım 2004.

AKVARYUMA HOŞGELDİNİZ

Aşağıda okuyacaklarınız, çoğumuzun işyerimizde, alışveriş yaparken ya da arabamızla bir yerden bir yere giderken sıradan bir günde yaşadıklarımızın kısa bir özeti. Gün içinde tüm bunları yaparken birileri tarafından izlendiğinizi hiç hissetmiyorsanız, bu yazıyı okuyunca düşünceleriniz değişebilir.



Yeni başlayacağınız yoğun bir iş günü için bilgisayarınızın başına oturdunuz. Önce işyerindeki e-posta hesabınıza gönderilen e-postalarınızı okuyup, göndermeniz gereken e-postaları gönderip, işinize daha sonra başlamaya karar verdiniz. Bilgisayarınızı açıp İnternet'e bağlandınız ve bir kaç e-posta okuyup gönderdiniz. Daha sonra birkaç web sitesini ziyaret ettiniz. İşyerinizdeki bilgisayarınız İnternet'e yüksek hızlı bir kablo modem yoluyla bağlı. Bina içinde başka birimdeki bir işinizi yapmak için yerinizden kalktınız. Bu sırada arkanızda bıraktığınız bilgisayarınızda İnternet bağlantınızı açık bıraktınız. **VERİLER NEREYE GİDİYOR:** İnternet Servis Sağlayıcınız (Internet Service Provider-ISP) size gelen ve sizin gönderdiğiniz e-postaları kendisine ait ana sunucularında saklar. Bağlı olduğunuz servis sağlayıcı şirketin verileri bellekte tutma politikasına göre, e-postalarınıza ait bilgiler birkaç saatliğine ya da birkaç yıl boyunca ana sunucularda saklanır. **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** İnternet Servis Sağlayıcı'nız ziyaret ettiğiniz web sitelerine ve alıp gönderdiğiniz e-postalara ait tüm bilgileri, resmi makamlara teslim etmeye zorlanabilir.



İşyerinizden ayrılıp kısa bir süre için başka bir yere gitmeniz gerekti. Arabanıza binerek yola çıktınız. Yolunuzun üstündeki ücretli geçiş gişelerinden geçerken arabanızın ön camına yapıştırmış olduğunuz radyo frekanslı tanıma sistemine yanıt veren otomatik geçiş etiketini kullandınız. **VERİLER NEREYE GİDİYOR:** Arabanızla gişeden geçtiğiniz kesin saat ve tarih bilgisinin, otomatik geçiş etiketinize bağlı olarak size tanımlanmış olan hesabınızda kaydı tutuluyor. Bu veri otomatik geçiş sistemini yönetmekle sorumlu yerel devlet kurumlarının bilgisayarlarında saklanıyor. **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** Gişelerden geçiş zamanınızı ve tarihinizi kesin olarak gösteren bilgiler, boşanma davaları da dahil olmak üzere, tüm mahkemelerde delil olarak kullanılabilir.

Arabanızla giderken yol kenarında bir kapkaç olayı gördünüz ve yanınızda bulunan cep telefonunuzdan polis imdat servisine ait numarayı çevirdiniz. Cep telefonu operatörünüze ait kulelerdeki özel alıcılar, aramanız sonucunda telefonunuzdan gönderilmiş olan sinyalin kendilerine ne kadar sürede ulaştığını hesapladılar ve kapsadıkları alanı, üçgenlere bölme yöntemiyle bulunduğunuz konumu belirleyerek bu bilgiyi polise gönderdiler. **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** Teknoloji kullanıcılarının sahip oldukları herhangi bir telefonun konumunu kesin bir doğrulukla izlemelerini sağlayan servisler sunuyor.

Öğle yemeğinizi yemek için yol kenarında bir lokantada durdunuz. Yemeğinizi yediniz ve hesabı kredi kartınızla ödemek için, garsona kredi kartınızı verdiniz. Ama garson, kartınızın manyetik alanını dolandırıcılık için özel olarak tasarlanmış bir düzenekten geçirerek, kartınızın arka yüzündeki manyetik bantta yer alan tüm bilgileri kopyaladı. Bu bilgiler daha sonra sayısız kez kopyalanarak çoğaltılacak ve satıldığında kolaylıkla nakit kazanç elde edilmesini sağlayacak elektronik ürünler satın almada kullanılacak. **VERİLER NEREYE GİDİYOR:** Dünya üzerinde neredeyse her yere gidebilir. Kredi kartı bilgileri İnternet üzerinden çabucak ve kolaylıkla satılabilir. Bu tür verileri kullanan hırsızlık şebekeleri Rusya'dan Endonozeya'ya kadar her yerde bulunmakta. **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** Kredi kartı ve kimlik bilgileri hırsızlığı en hızlı büyüyen suç türlerinden biri. 2002 yılında her yirmi ABD vatandaşından biri bu suçtan etkilenmiş.

Yemek yediğiniz lokantada kablosuz İnternet bağlantısı olanağı olduğunu gördünüz ve biraz İnternet'te gezinmek için yanınızdaki dizüstü bilgisayarınızı açtınız. Çalıştığınız şirketteki bilgisayarınızda, klavyede bastığınız her bir tuşu, girdiğiniz her bir web sitesini ve okuduğunuz her bir e-postayı kaydeden bir uzaktan izleme yazılımı kurulu olduğundan haberiniz yok. **VERİLER NEREYE GİDİYOR:** Bu bilgiler otomatik olarak işyerindeki paranoyak bir müdüre ya da kıskanç bir eşe e-posta yoluyla gönderilebilir! **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** Bir bilgisayarda yapılan tüm işlemlerin izlenmesini sağlayan yazılımlar oldukça ucuz ve yaygın. Bu sinsice izleme teknolojisi, farkedilmesi çok güç bir şekilde arka tarafta gizlice çalışıyor.

Dönüşte, evinizdeki birkaç eksiği ve aylık "Bilim ve Teknik" derginizi satın almak amacıyla bir süpermarkete uğradınız. Ödeme yapmak için kasaya geldiğinizde bu süpermarkete ait müşteri kartınızı kullandınız ve ödemenizi %5 indirimli olarak yaptınız. Tebrikler! **VERİLER NEREYE GİDİYOR:** Çok sayıda şubesi olan zincir mağazalar, kasada müşteri kartı kullanarak ödeme yapan müşterileri tarafından yapılan tüm alışverişleri kaydediyor ve daha sonra bu bilgileri mağazanın ana veri işleme merkezine iletiyor. Bu merkezde yapılan alışverişe ilişkin tüm bilgiler, müşterinin adı soyadı, adresi ve telefon numarasıyla bağlantısı kurulmuş bir dosya içinde saklanıyor. Bu dosyalar kasada ödeme yaptığınız sırada ya da mağazanın bu bilgileri göstermek istediği herhangi bir kişi tarafından izlenebilir. Bu kişi mağaza satış pazarlama görevlisi olabileceği gibi polis de olabilir. **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** Satın aldığınız her şeyin bilgisini birilerinin elinde tutmasını gerçekten ister misiniz? Bunu bir kez daha düşünün.

Satın almanız gereken birçok farklı şey olduğunu, süpermarketin yeterli gelmediğini farkettiniz ve büyük bir alışveriş merkezine gitmeye karar verdiniz. Alışveriş merkezinin koridorlarında gezinirken çevreye yerleştirilmiş olan 250 adet akıllı gözetleme kamerasından biri size kilitlendi ve siz bloklar boyunca ilerledikçe sizi izlemeyi sürdürdü. Kameraları kontrol eden bilgisayarlar "şüpheli" davranışları belirlemeye programlanmıştı. Şüpheli bir davranışta bulunursanız kameradaki görüntünüz renklendirilerek belirginleştirilecek ve polise iletilecek. **VERİLER NEREYE GİDİYOR:** Acil durum servislerine, polise, FBI ve CIA gibi devletin haber alma kurumlarına.

Dışarıda yapmanız gerekenleri bitirip akşam işyerinize döndünüz ve bütün gün boyunca İnternet'e bağlı kalmış olan bilgisayarınızın başına oturdunuz. Son ödeme günü gelmiş bazı faturalarınızı ödemek için hesaplarınızın bulunduğu bankanın İnternet bankacılığı bölümüne girdiniz ve ödemelerinizi yaptınız. Bunları yaparken, bilgisayarınızın başında olmadığınız süre boyunca bilgisayar korsanlarının sisteminiz üzerine üç tane casus yazılımı kurduğunu farketmediniz bile. **VERİLER NEREYE GİDİYOR:** Casus yazılımları İnternet'ten ücretsiz olarak indirilebiliyor, yani bu yazılımları herkes kolaylıkla yayabilir. Bu yazılımlar parolaları ve kredi kartına ilişkin ayrıntılı bilgileri ele geçirebilir ya da birilerinin bilgisayarınızı virüslü e-postalar ya da müstehcen içerikli dökümanlar dağıtacak şekilde dilediği gibi kullanmasını olanaklı kılabilir. **ENDİŞELENMEK İÇİN NEDENLERİNİZ:** Web'de gezinen yaklaşık 25.000 casus programı var. Yapılan yeni bir çalışma evlerde kullanılan geniş bant bağlantı hızıyla İnternet'e bağlı olan kişisel bilgisayarların %80'inin casus yazılımlardan etkilendiğini gösteriyor.