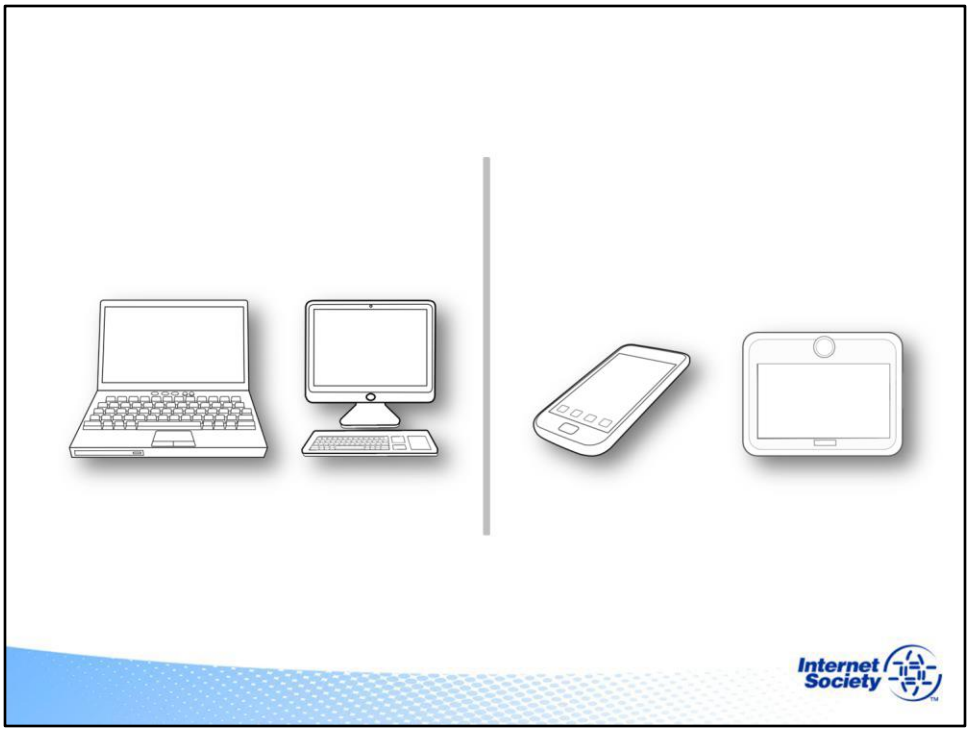
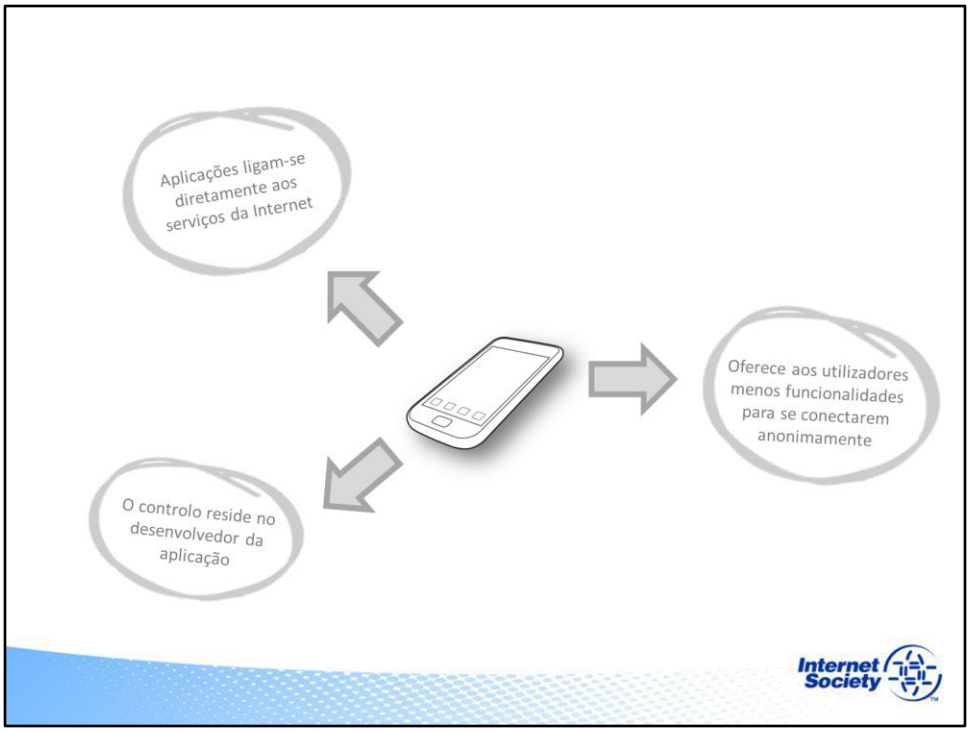
Bem-vindo a Pegadas Digitais, módulo cinco.
Neste módulo, aprenderemos as maneiras pelas quais diferentes dispositivos podem deixar pegadas digitais diferentes.

Estes são o Samuel e a Ana. O Samuel gosta de trabalhar no seu portátil, enquanto Ana está sempre colada ao seu *smartphone*.
Posto isto, será que eles deixam diferentes tipos de pegadas digitais enquanto utilizadores da Internet? Vamos descobrir.



Os *smartphones* e *tablets* tendem a deixar uma pegada muito diferente dos portáteis e computadores de mesa.

Os *smartphones* modernos funcionam de forma a deixar uma pegada mais intrusiva.

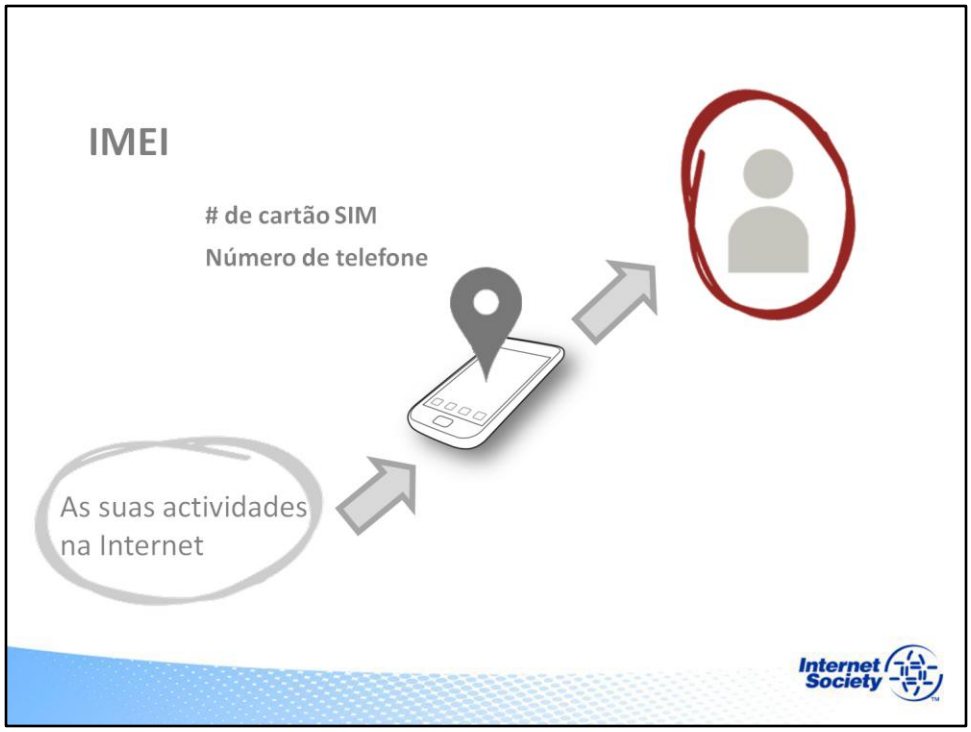


As aplicações ligam-se diretamente aos serviços da Internet usando interfaces específicas. O controlo sobre quais informações são enviadas para outros serviços / dispositivos fica nas mãos de quem desenvolveu a aplicação e o utlizador dispõe somente do controlo que o programador permitiu. Os dispositivos móveis, particularmente, oferecem aos utilizadores menos funcionalidades para se conectarem anonimamente.

Os *smartphones* geralmente têm geo-localização. Isso possibilita que os serviços marquem as suas atividades com o local geográfico onde se encontra. Os serviços de localização geralmente são habilitados por omissão ou incluídos num pacote de permissões que o utilizador é solicitado a conceder quando uma aplicação é instalada.

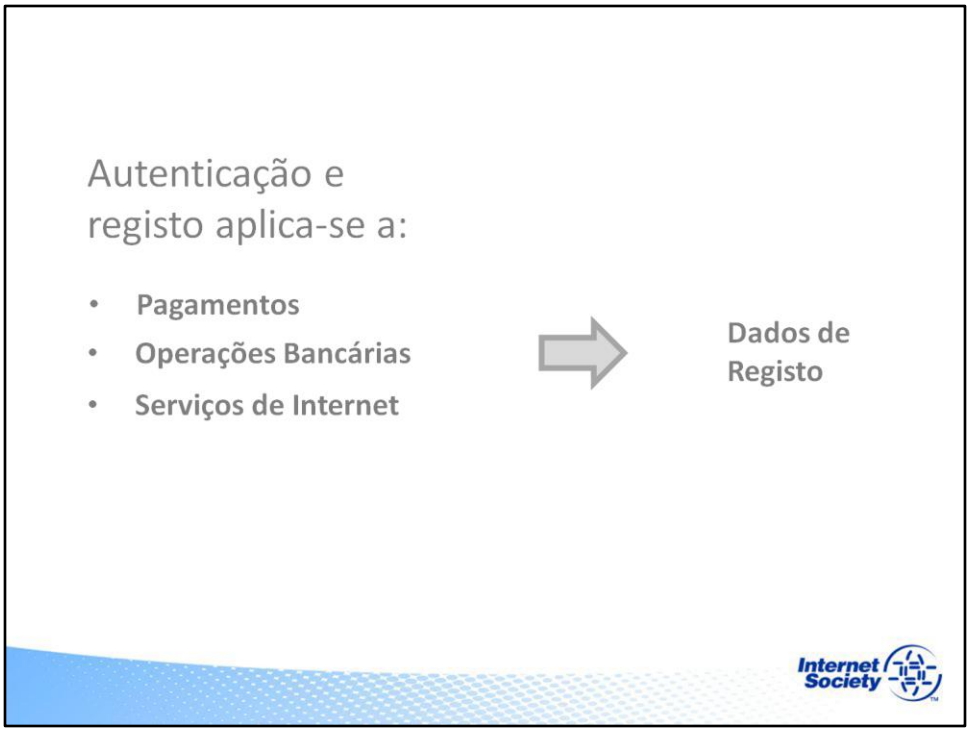
Os dados de localização podem ser partilhados explicitamente, se a aplicação obtiver os seus dados de localização e enviá-los ao serviço de Internet, ou implicitamente - por exemplo, se as fotos e os vídeos que carregar foram marcados com o local, a data e a hora em que foram tirados.

Acredita-se que entre 4-6 itens de dados de localização sejam suficientes para identificar qualquer utilizador em particular.



Os *smartphones* são conceptualizados como dispositivos muito pessoais e contêm vários identificadores exclusivos, nomeadamente o IMEI (*International Mobile Station Equipment Identity*), o número de série do cartão SIM, o número de telefone em si, é claro, e recentemente também um endereço MAC, identificador *Bluetooth* e por aí em diante. A sua operadora de serviços móveis pode correlacionar todos os seus dados de assinante (nome, endereço, detalhes de pagamento, etc.) a todas as suas atividades na Internet, ligando o mundo físico ao virtual.

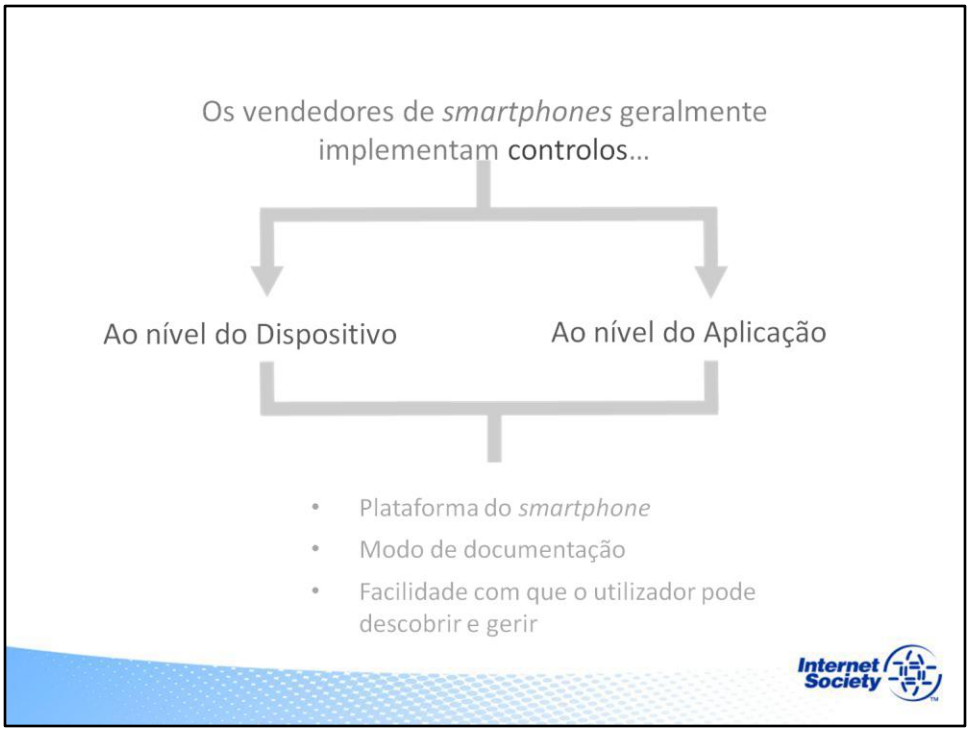
Como agora muitos países exigem algum tipo de identificação para registar todos os assinantes de telemóveis, torna-se simples para terceiros, como agências policiais, correlacionar a atividade da Internet a um *smartphone* específico e, por conseguinte, a um utilizador individual.



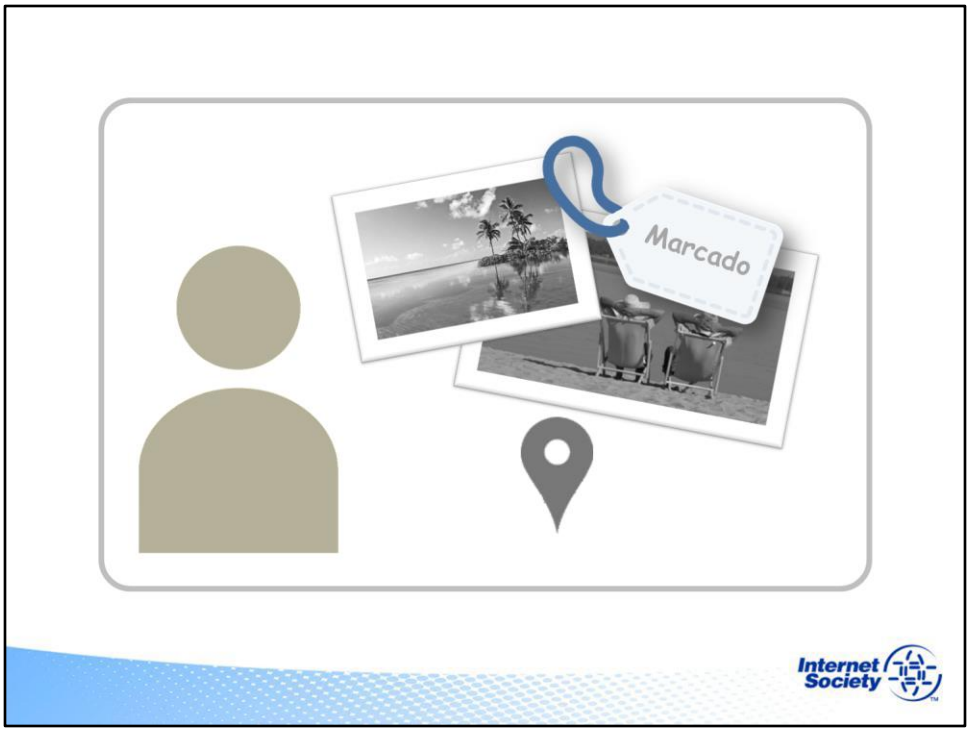
Os dispositivos móveis não são únicos no que toca a identificação de assinantes. O mesmo princípio no sentido da autenticação e registo aplica-se também aos serviços de pagamento, operações bancárias e de Internet, facilitando a correlação entre as atividades *online* e as do mundo real para quem tem acesso aos dados de registo.

O que pode então distinguir os dois casos é até que ponto as leis de um país controlam o comportamento dos provedores de serviços. Isso pode existir na forma de regulamentos de privacidade que se aplicam a um setor específico (por exemplo, serviços financeiros) ou ao uso de dados de identificação pessoal, independentemente do setor envolvido.

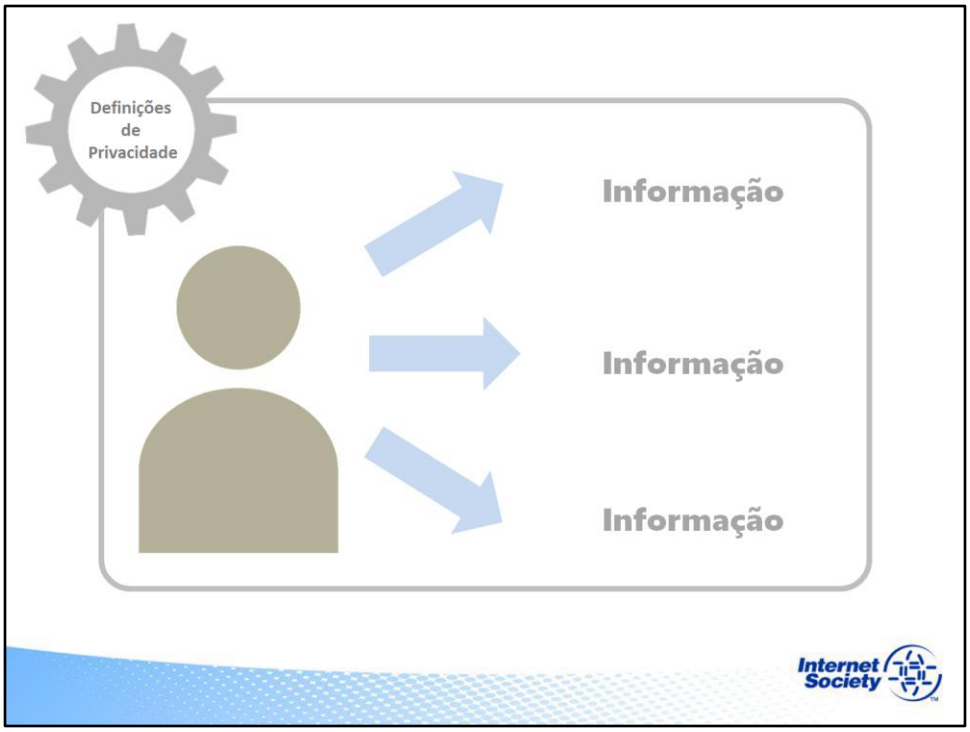
Os vendedores de *smartphones* geralmente implementam controlos sobre a partilha de dados de localização e bloqueiam a utilização de identificadores específicos a dispositivos pelas aplicações. Este é um aspeto que está normalmente fora do controlo do utilizador.



Alguns controlos sobre informações confidenciais, no entanto, são baseados em configurações ao nível do dispositivo e outros ao nível da aplicação. Essas funcionalidades variam significativamente de acordo com a plataforma do *smartphone*; o mesmo se aplica ao modo como estão documentadas e a facilidade com que o utilizador comum pode descobri-las e fazer a sua gestão.



Porém, quando um utilizador começa a tirar fotos marcadas ou dá permissão a uma aplicação recém-instalada para ver informações de localização, a permissão concedida à aplicação é raramente revista.

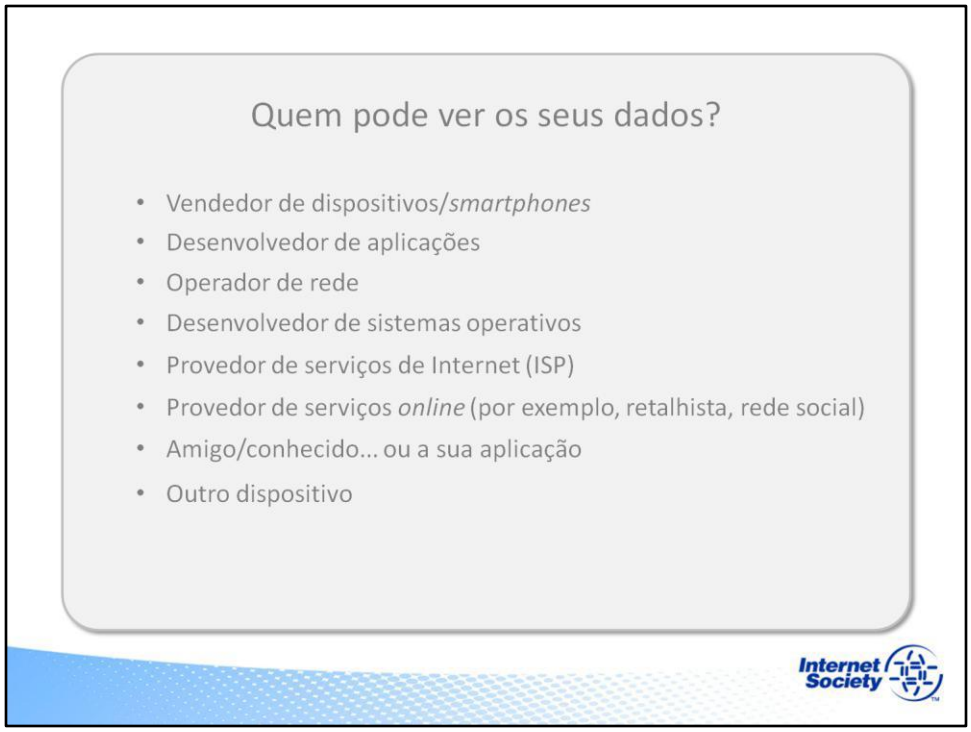


Mesmo um consumidor diligente que verifica regularmente as definições de privacidade está partilhar mais informações do que permitiu.

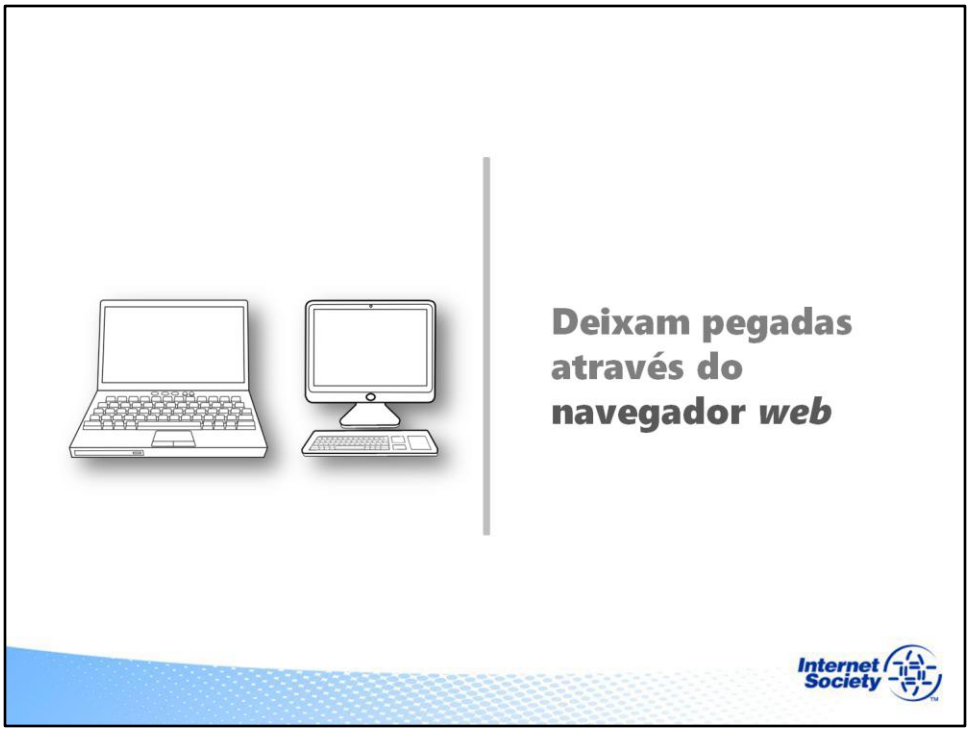
Por exemplo, simplesmente ligar um telemóvel permite que a operadora localize o telefone com um certo grau de precisão. E se alguém o "marcar" numa fotografia que foi carregada para uma rede social, a sua localização numa data e hora específica acabou de ser partilhada na Internet pelos seus amigos - mesmo que o seu próprio *smartphone* esteja desligado e pousado na mesa da cozinha em casa.

Em alguns casos, o vendedor do dispositivo pode ter acesso a informações confidenciais e privadas no *smartphone*.

A privacidade de um indivíduo pode ser afetada pelas ações de muitas outras entidades. Clique no *smartphone* para visualizar uma lista de entidades que podem afetar a privacidade de um indivíduo enquanto estiver a usar um dispositivo móvel.



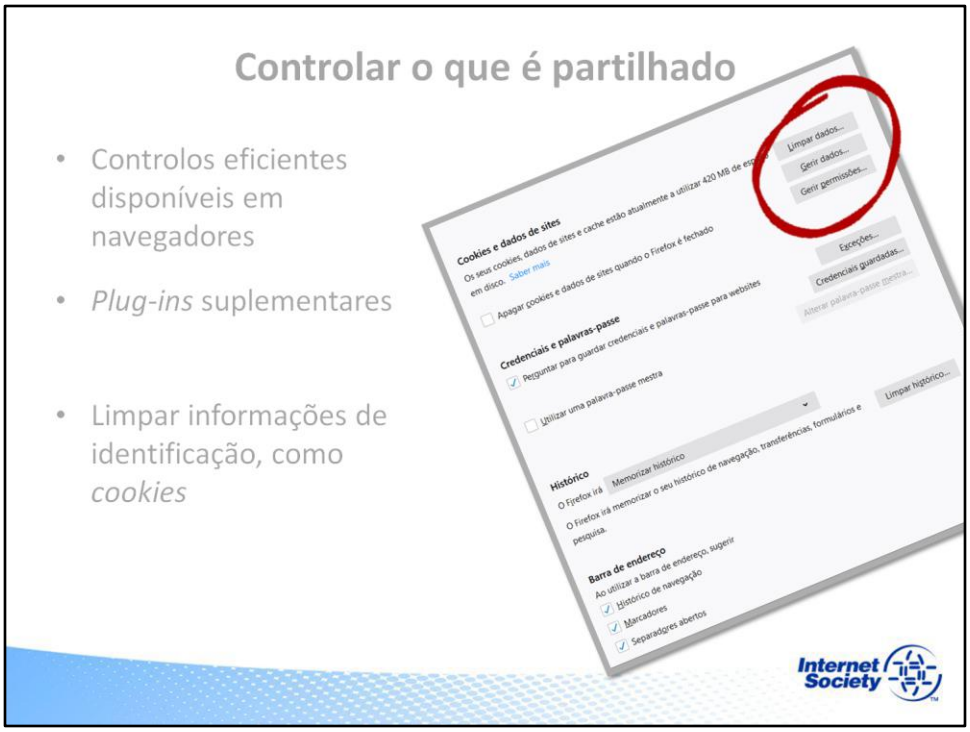
Eis uma lista apenas do cenário de utilização de dispositivos móveis: vendedor de dispositivos/smartphones, desenvolvedor de aplicações, operador de rede, desenvolvedor de sistemas operativos, provedor de serviços de Internet (ISP), provedor de serviços *online* (por exemplo, retalhista, rede social), amigo/conhecido... ou sua aplicação e/ou outro dispositivo.
Clique em "Avançar" para continuar.



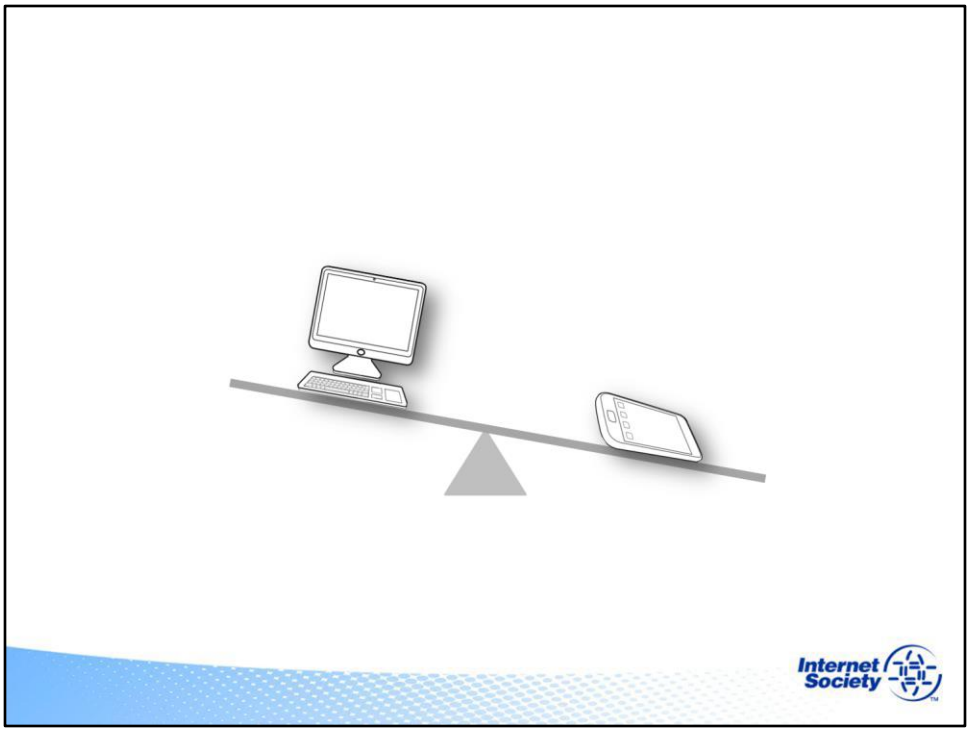
Agora, vamos ver como as pegadas deixadas para trás na utilização de computadores ou portáteis diferem dos *smartphones*.

Os utilizadores de computadores de mesa e portáteis deixam principalmente pegadas pelo navegador *web*.

O navegador da *Web* padrão é muito diferente das aplicações utilizadas em *smartphones* e *tablets*.



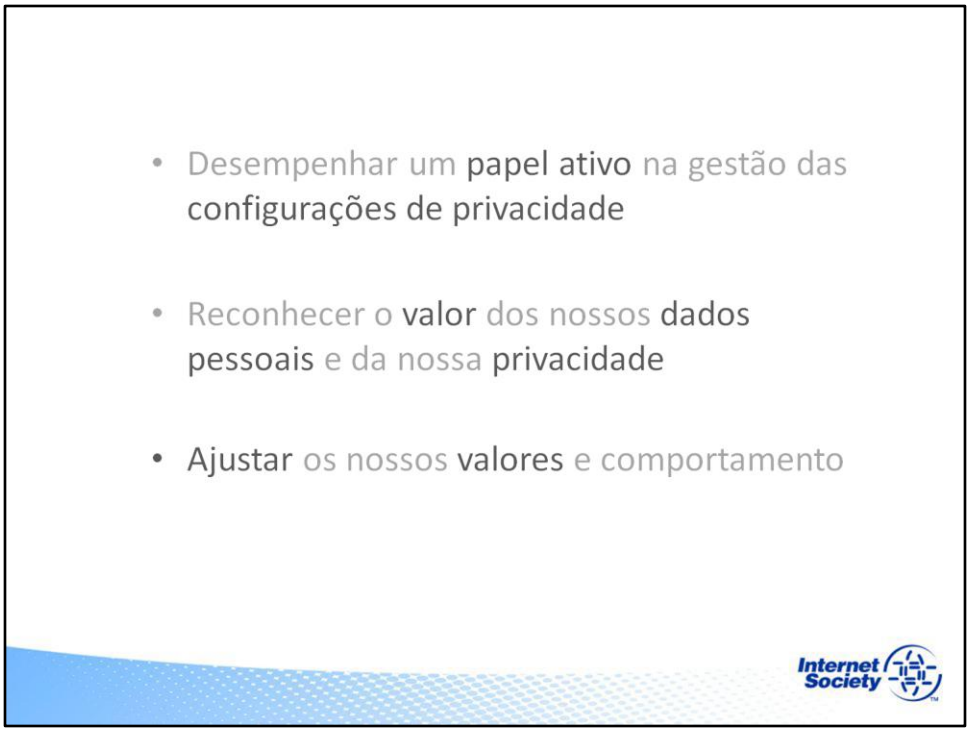
Os controlos relativamente eficientes disponibilizados pelos próprios navegadores ou por *plug-ins* suplementares facilitam o controlo do que é partilhado pelo utilizador final e limpam informações de identificação, como *cookies*, que de outra forma poderiam reduzir a privacidade pessoal.



Assim, actualmente, os computadores de mesa têm uma vantagem no que toca à privacidade em relação aos *smartphones*. Mas não serão capazes de mantê-la por muito tempo.

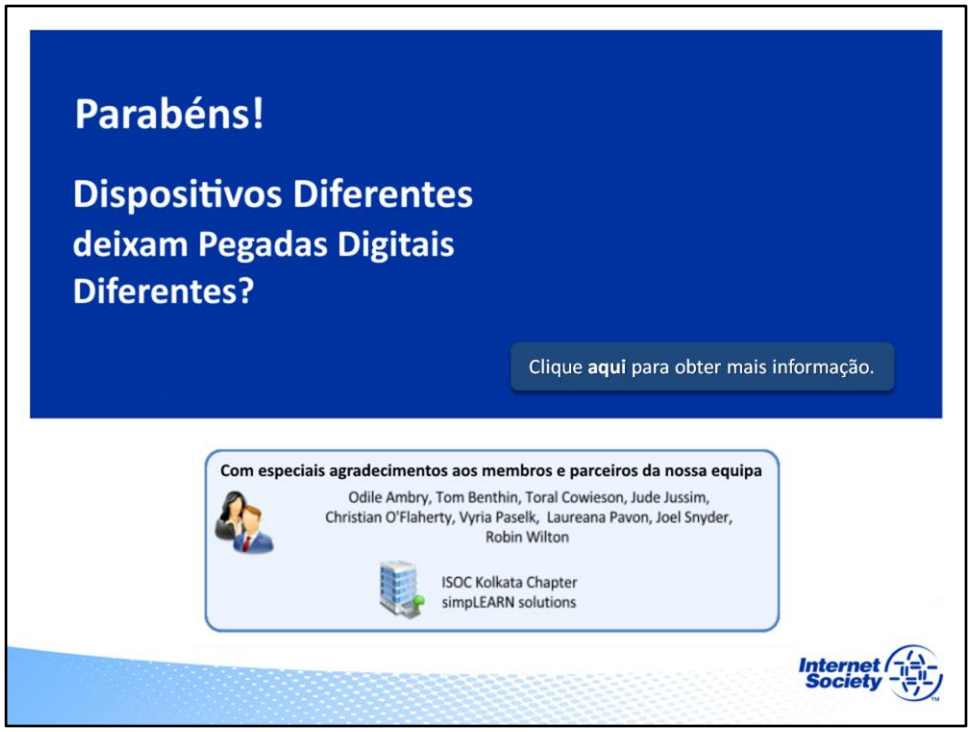
À medida que as expectativas dos utilizadores são cada vez mais impulsionadas pela experiência de *smartphones/tablets*, existe uma pressão para sistemas operativos como o Windows 10 se comportarem mais como um *smartphone* do que como um computador de mesa 'tradicional' - com a mesma perda potencial de controlo e privacidade do utilizador.

Internautas preocupados com as pegadas digitais deixadas pelos seus *smartphones*...



... Precisam de desempenhar um papel ativo na gestão das suas configurações de privacidade.

A tarefa de monitorizar e controlar cuidadosamente a privacidade representa uma sobrecarga significativa e pode ser mais complexa do que muitos utilizadores de *smartphones* esperam. O desafio para todos nós, como consumidores e utilizadores, passa por reconhecer o valor das nossas informações pessoais e da nossa privacidade: apenas através de um ajuste aos nossos valores e, por conseguinte, o nosso comportamento, podemos esperar tomar decisões melhores e sustentáveis sobre privacidade.



Parabéns! Completou Pegadas Digitais, módulo cinco - Dispositivos Diferentes deixam Pegadas Digitais Diferentes?
Lembramos que pode sempre encontrar mais informação, documentação técnica e outros módulos de formação através das páginas sobre Identidade e Privacidade da Internet Society.
http://www.eprivacidade.pt/recursos/tutorial-privacidade/index.html