



Control use of data to protect privacy

(Landau, 2015)

Filipe Cordeiro de Medeiros Azevêdo



Fair Information Practices (FIPs)

Desenvolvido na década de 60 em resposta ao crescimento de sistemas computacionais

Os 5 princípios fundamentais da proteção da privacidade:

- Anúncio
- Acesso
- Consentimento
- Corretude
- Integridade e segurança



As permissões de uso não foram feitas para humanos



As permissões de uso não foram feitas para humanos

Estudo mostra que um leitor levaria em média 244 horas para ler todas as políticas de privacidade dos serviços que utiliza em 1 ano.

(A. M. McDonald et al, 2008)

Consentimento não é realístico dado a complexidade e número de decisões que precisam ser feitas pelos usuários



Exemplos

- Google market
- Target
- Uber
- Amazon e-book
- NSA

Permissões de uso do Facebook App

Este app tem acesso a:



Histórico do dispositivo e apps

- recuperar apps em execução



Identidade

- encontrar contas no dispositivo
- adicionar ou remover contas
- ler próprio cartão de contato



Agenda

- ler compromissos e informações confidenciais
- adicionar ou modificar compromissos e enviar e-mail para os convidados sem o conhecimento dos donos



Contatos

- encontrar contas no dispositivo
- ler seus contatos
- modificar seus contatos
- ler registro de chamadas
- ler status e identidade do telefone
- salvar no registro de chamadas



Fotos/mídia/arquivos

- ler conteúdo do armazenamento USB
- alterar ou excluir conteúdo de armazenamento USB



Armazenamento

- ler conteúdo do armazenamento USB
- alterar ou excluir conteúdo de armazenamento USB



Câmera

- tirar fotos e gravar vídeos



Microfone

- gravar áudio



Informações de conexão Wi-Fi

- ver conexões Wi-Fi



Informações de chamada e código do dispositivo

- ler status e identidade do telefone



Outras



Outras

- fazer download de arquivos sem notificação
- ajustar tamanho do plano de fundo
- receber dados da Internet
- ver conexões de rede
- criar contas e definir senhas
- acessar estatísticas da bateria
- enviar transmissão persistente
- alterar conectividade da rede
- conectar e desconectar do Wi-Fi
- expandir/recolher barra de status
- acesso total à rede
- alterar suas configurações de áudio
- ler as configurações de sincronização
- executar na inicialização
- reorganizar os apps em execução
- definir plano de fundo
- sobrepor outros apps
- impedir modo de suspensão do dispositivo
- ativar e desativar sincronização
- instalar atalhos
- ler a configuração de serviço do Google



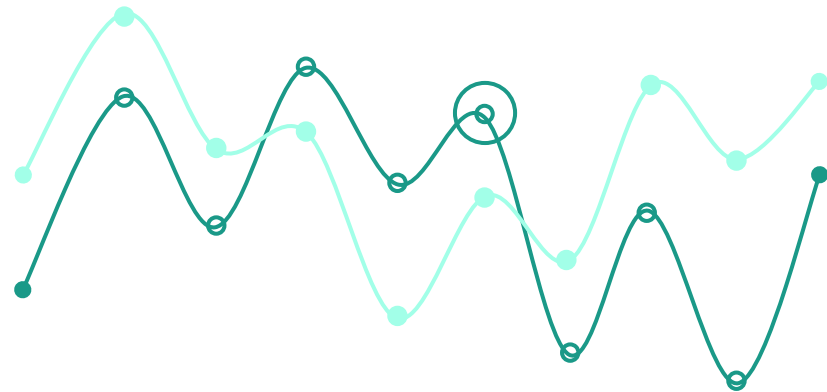
Contra exemplos

- Shibboleth
- Account HTTP



Controlando o uso dos dados

Tecnologia, política e legislação



Controlando o uso dos dados

“É necessário redefinir de tempos em tempos a natureza e extensão exata da proteção da privacidade”
(Warren e Brandeis - 1890)

The Camera to Buy,

That is, if Photography means to you anything more than the fancy of a passing moment — is, without doubt,

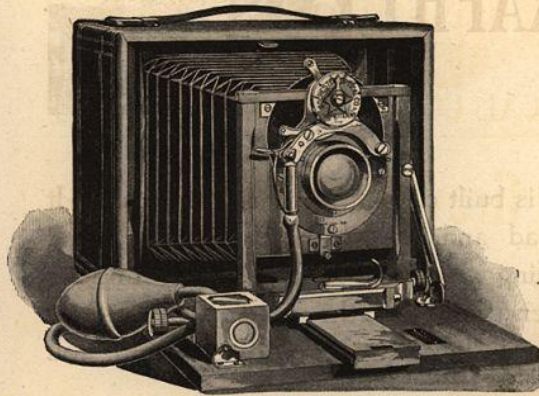
THE . . .

PREMO.


With the widest range of subjects, in the simplest manner possible, it produces, uniformly, the very best results.

Send for copy of Premo catalogue free. Will send sample photograph for five cents in stamps.

Rochester Optical Co.,
47 SOUTH ST.,
Rochester, N. Y.



[K0545] \$10 to \$50.



What the “right to be forgotten” means for privacy in a digital age

(Newman et al, 2015)

O direito de ser esquecido

- Iniciado na europa, em maio de 2014





Problema na análise de crédito

- Aproximadamente 100% da população americana possui registro de análise de crédito no setor privado
- A Federal Trade Commission realizou um estudo em 2012 e descobriu que 25% da população possui algum erro nos registros da análise de crédito
- Experian produz um grande número de análises de crédito com erro e clientes tem grande dificuldade em corrigí-los



Diferentes abordagens

- Estados Unidos = Coleta dos dados
- Europa = Uso dos dados



Conclusão

O “direito de ser esquecido” não é uma solução completa, mas é uma importante ferramenta para a garantia do direito à privacidade, atuando no controle do uso dos dados.

