# Chapter 2 Privasi

## 2.1 Risiko dan Prinsip Privasi

**2.1.1 Apa Apakah Privasi?**

Setelah jatuhnya pemerintah komunis di Jerman Timur, orang-orang memeriksa file-file Stasi, polisi rahasia. Mereka menemukan bahwa pemerintah telah menggunakan mata-mata dan informan untuk membuat catatan rinci tentang pendapat dan kegiatan sekitar enam juta orang - sepertiga dari populasi. Informan adalah tetangga, rekan kerja, teman, dan bahkan anggota keluarga dari orang-orang yang mereka laporkan. File-file kertas mengisi sekitar 125 mil dari ruang rak.

Sebelum era digital, kamera pengintai mengawasi pembeli di bank dan toko. Dan dalam era komputer dan Internet, apotek di Indiana membuang ratusan resep, tanda terima, dan formulir pemesanan obat-obatan dengan membuangnya ke tempat sampah terbuka. Investigator swasta masih mencari sampah rumah tangga untuk informasi medis dan keuangan, rincian pembelian, bukti hubungan romantis, dan jurnalis

catatan.

Teknologi komputer tidak diperlukan untuk invasi privasi. Namun, kami mendiskusikan privasi secara panjang lebar dalam buku ini karena penggunaan teknologi digital telah membuat ancaman baru menjadi mungkin dan ancaman lama menjadi lebih kuat. Teknologi komputer — basis data, kamera digital, Web, smartphone, dan perangkat sistem pemosisian global (GPS), antara lain — telah sangat mengubah apa yang dapat diketahui orang tentang kita dan bagaimana mereka dapat menggunakan informasi tersebut. Memahami risiko dan masalah adalah langkah pertama menuju perlindungan privasi. Untuk profesional komputer, memahami risiko dan masalah adalah langkah menuju perancangan sistem dengan perlindungan privasi built-in dan risiko yang lebih kecil.

Ada tiga aspek kunci dari privasi :

* Kebebasan dari intrusi — dibiarkan sendiri
* . Kontrol informasi tentang diri sendiri
* . Kebebasan dari pengawasan (dari diikuti, dilacak, diawasi, dan disadap)

Untuk sebagian besar, dalam buku ini, kita memandang privasi sebagai hal yang baik. Para kritikus privasi berpendapat bahwa hal itu memberikan perlindungan terhadap penipuan, kemunafikan, dan kesalahan. Ini memungkinkan penipuan. Ini melindungi orang yang bersalah. Kepedulian terhadap privasi dapat dianggap dengan kecurigaan "Apa yang harus Anda sembunyikan?" Keinginan untuk menjaga hal-hal pribadi tidak berarti kita melakukan sesuatu yang salah. Kami mungkin ingin menjaga kesehatan, hubungan, dan masalah keluarga pribadi. Kami mungkin ingin menjaga keyakinan agama dan pandangan politik pribadi dari beberapa orang yang berinteraksi dengan kami. Privasi beberapa jenis informasi dapat menjadi penting untuk keselamatan dan keamanan juga. Contohnya termasuk rencana perjalanan, data keuangan, dan untuk beberapa orang, cukup alamat rumah.

Ancaman privasi datang dalam beberapa kategori:

* Penggunaan informasi pribadi yang disengaja dan institusional (di sektor pemerintah terutama untuk penegakan hukum dan pengumpulan pajak, dan di sektor swasta terutama untuk pemasaran dan pengambilan keputusan)
* Penggunaan atau pelepasan yang tidak sah oleh “orang dalam,” orang-orang yang menjaga informasi
* Pencurian informasi
* Kebocoran yang melalui kelalaian atau kecerobohan
* Tindakan kita sendiri (kadang-kadang yang disengaja dan terkadang ketika kita tidak menyadari risiko)

Masalah privasi muncul di banyak konteks. Lebih banyak topik dengan implikasi privasi muncul di bab-bab selanjutnya. Kami mendiskusikan spam, intrusi email sampah dan pesan teks, di Bab 3.Kami membahas peretasan dan pencurian identitas di Bab 5.Kami membahas pemantauan komunikasi di tempat kerja dan masalah privasi lainnya bagi karyawan di Bab 6. Beberapa risiko privasi dihasilkan dari Fakta bahwa begitu banyak data yang disimpan tentang kita salah. Database mengandung kesalahan. File tidak diperbarui. Rekaman orang-orang yang berbeda dengan nama-nama yang mirip atau kesamaan lainnya menjadi bingung atau bingung. Bab 8 membahas beberapa masalah ini. Privasi muncul lagi di Bab 9, di mana kami fokus pada tanggung jawab

profesional komputer.

Jelas bahwa kita tidak dapat mengharapkan privasi lengkap. Biasanya kami tidak menuduh seseorang yang memulai percakapan untuk melanggar privasi kami. Banyak teman dan sedikit kenalan tahu seperti apa Anda, di mana Anda bekerja, mobil jenis apa yang Anda kendarai, dan apakah Anda orang yang baik. Mereka tidak perlu mendapatkan izin Anda untuk mengamati dan berbicara tentang Anda. Pengendalian informasi tentang diri sendiri berarti mengendalikan apa yang ada dalam pikiran, ponsel, dan sistem penyimpanan data orang lain. Itu harus dibatasi oleh hak asasi manusia, terutama kebebasan berbicara. Kami juga tidak bisa berharap untuk benar-benar bebas dari pengawasan. Orang melihat kita dan mendengar kita ketika kita bergerak di depan umum (secara fisik atau di Web).

Jika Anda tinggal di kota kecil, Anda memiliki sedikit privasi; semua orang tahu segalanya tentangmu. Di kota besar, Anda hampir anonim. Tetapi jika orang tidak tahu apa-apa tentang Anda, mereka mungkin mengambil risiko besar jika mereka menyewakan Anda tempat tinggal, mempekerjakan Anda, meminjamkan uang kepada Anda, menjual asuransi mobil, menerima kartu kredit Anda, dan sebagainya. Kami menyerahkan beberapa privasi untuk manfaat berurusan dengan orang asing. Kita dapat memilih untuk menyerah lebih banyak sebagai imbalan atas manfaat lain seperti kenyamanan, layanan yang dipersonalisasi, dan komunikasi yang mudah dengan banyak teman. Tetapi terkadang, yang lain membuat pilihan untuk kita.

Saya menggunakan banyak kejadian nyata, bisnis, produk, dan layanan sebagai contoh di seluruh buku ini. Dalam banyak kasus, saya tidak memilih mereka untuk mendapat dukungan atau kritik khusus. Mereka hanyalah beberapa dari banyak contoh yang dapat kita gunakan untuk mengilustrasikan masalah, masalah, dan solusi yang mungkin.

*Orang yang dipaksa untuk hidup setiap menit dari kehidupannya di antara*

*orang lain dan yang setiap kebutuhan, pikiran, keinginan, kesenangan atau kepuasannya*

*tunduk pada pengawasan publik, telah kehilangan individualitas*

*dan martabat manusia. [Dia] menyatu dengan massa. . . . Makhluk seperti itu,*

*meskipun hidup, adalah fungible; dia bukan seorang individu.*

—Edward J. Bloustein2

*Penting untuk menyadari bahwa privasi tidak melindungi rahasia pribadi, tetapi*

*rasa aman dalam lingkaran teman-teman sehingga individu dapat*

*lebih jujur, lebih ekspresif, lebih* terbuka *dengan "rahasia."*

—Robert Ellis Smith

### 2.1.2 Teknologi Baru, Risiko Baru

Komputer, Internet, dan seluruh larik perangkat digital — dengan peningkatan kecepatan, ruang penyimpanan, dan konektivitasnya yang luar biasa — membuat koleksi, penelusuran, analisis, penyimpanan, akses, dan distribusi besar jumlah informasi dan gambar jauh lebih mudah, lebih murah, dan lebih cepat daripada sebelumnya. Ini adalah manfaat yang luar biasa. Tetapi ketika informasi itu tentang kita, kemampuan yang sama mengancam privasi kita.

Saat ini ada ribuan (mungkin jutaan) dari database, baik pemerintah maupun swasta, yang berisi informasi pribadi tentang kami. Di masa lalu, tidak ada catatan tentang beberapa informasi ini, seperti pembelian barang kebutuhan sehari-hari dan buku-buku kami. Dokumen pemerintah seperti perceraian dan catatan kebangkrutan telah lama ada di catatan publik, tetapi mengakses informasi tersebut membutuhkan banyak waktu dan upaya. Ketika kita melihat-lihat di perpustakaan atau toko, tidak ada yang tahu apa yang kita baca atau lihat. Itu tidak mudah untuk menghubungkan bersama catatan keuangan, pekerjaan, dan keluarga kami. Sekarang, perusahaan besar yang mengoperasikan video, email, jejaring sosial, dan layanan pencarian dapat menggabungkan informasi dari penggunaan anggota mereka semua untuk mendapatkan gambaran terperinci tentang minat, opini, hubungan, kebiasaan, dan aktivitas orang tersebut. Bahkan jika kita tidak masuk sebagai anggota, perangkat lunak melacak aktivitas kita di Web. Di masa lalu, percakapan menghilang ketika orang selesai berbicara, dan hanya pengirim dan penerima biasanya membaca komunikasi pribadi. Sekarang, ketika kita berkomunikasi dengan mengirim SMS, email, jejaring sosial, dan sebagainya, ada catatan kata-kata kita bahwa orang lain dapat menyalin, meneruskan, mendistribusikan secara luas, dan membaca bertahun-tahun kemudian. Miniaturisasi prosesor dan sensor menempatkan kamera kecil di ponsel yang jutaan orang bawa kemana-mana. Kamera di beberapa pesawat televisi 3-D memperingatkan anak-anak jika mereka duduk terlalu dekat. Apa lagi yang mungkin direkam kamera tersebut, dan siapa yang mungkin melihatnya? Peralatan nirkabel yang kami bawa berisi GPS dan perangkat lokasi lainnya. Mereka memungkinkan orang lain untuk menentukan lokasi kami dan melacak gerakan kami. Pasien mengisi ulang resep dan memeriksa hasil tes medis di Web. Mereka berkorespondensi dengan dokter melalui email. Kami menyimpan foto dan video kami, melakukan pajak, dan membuat serta menyimpan dokumen dan spreadsheet keuangan di cloud server jauh, bukan di komputer kami sendiri. Penyedia daya dan air mungkin segera memiliki sistem pengukuran dan analisis yang cukup canggih untuk menyimpulkan peralatan apa yang kita gunakan, ketika kita mandi (dan untuk berapa lama), dan ketika kita tidur. Lembaga penegak hukum memiliki alat yang sangat canggih untuk menguping, mengawasi, dan mengumpulkan serta menganalisis data tentang aktivitas orang, alat yang dapat membantu mengurangi kejahatan dan meningkatkan keamanan — atau mengancam privasi dan kebebasan.

Menggabungkan alat dan aplikasi baru yang kuat dapat memiliki hasil yang menakjubkan. Anda dapat mengambil foto seseorang di jalan, mencocokkan foto itu dengan seseorang di jejaring sosial, dan menggunakan data berisi informasi yang dapat diakses publik untuk ditebak, dengan kemungkinan akurasi tinggi, nama orang, tanggal lahir, dan sebagian besar nomor Jaminan Sosialnya.

Ini tidak membutuhkan superkomputer; itu dilakukan dengan aplikasi smartphone. Kami melihatsemacam itu sistem di acara-acara televisi dan film, tetapi bagi kebanyakan orang mereka tampak dilebih-lebihkan atau jauhpergi di masa depan.

Semua gadget, layanan, dan aktivitas ini memiliki manfaat, tentu saja, tetapi mereka memaparkan kita pada risiko baru. Implikasi untuk privasi sangat besar.

*Informasi medis pasien bersifat rahasia. Itu tidak boleh didiskusikan*

*di tempat umum.*

- Sebuah tanda, ditujukan untuk dokter dan staf, di lift dikantor medis

gedung, pengingat untuk mencegah kebocoran privasi berteknologi rendah.

**Contoh: Cari data kueri**

Setelah seseorang memasukkan frasa ke mesin telusur, melihat beberapa hasil, lalu melanjutkan ke tugas lain, dia berharap kalimat itu hilang — pergi seperti percakapan dengan teman atau beberapa kata yang diucapkan kepada seorang pegawai di toko. Lagi pula, dengan jutaan orang melakukan pencarian setiap hari untuk bekerja, sekolah, atau penggunaan pribadi, bagaimana perusahaan pencarian menyimpan semua itu? Dan siapa yang ingin semua informasi sepele itu? Itulah yang dipikirkan kebanyakan orang tentang pertanyaan pencarian sampai dua insiden menunjukkan bahwa itu memang disimpan, itu dapat dilepaskan, dan itu penting.

Mesin pencari mengumpulkan banyak terabyte data setiap hari. Terabyte adalah satu triliun byte. Akan sangat mahal untuk menyimpan banyak data di masa lalu, tetapi tidak lagi. Mengapa perusahaan mesin pencari menyimpan permintaan pencarian? Sangat menggoda untuk mengatakan "karena mereka bisa." Tapi ada banyak kegunaan untuk data. Misalkan, misalnya, Anda menelusuri “Milky Way.” Baik Anda mendapatkan banyak halaman astronomi atau informasi tentang candy bar atau restoran lokal dapat bergantung pada riwayat pencarian Anda dan informasi lain tentang Anda. Perusahaan mesin pencari ingin tahu berapa banyak halaman hasil pencarian yang dilihat pengguna, berapa banyak yang mereka klik, bagaimana mereka memperbaiki permintaan pencarian mereka, dan kesalahan ejaan apa yang biasanya mereka buat. Perusahaan menganalisis data untuk meningkatkan layanan pencarian, untuk menargetkan iklan lebih baik, dan mengembangkan layanan baru. Database dari query yang lalu juga menyediakan input yang realistis untuk menguji dan mengevaluasi modifikasi dalam algoritma yang digunakan mesin pencari untuk memilih dan memberi peringkat hasil. Data permintaan pencarian berharga bagi banyak perusahaan selain perusahaan mesin pencari. Dengan menganalisis permintaan pencarian, perusahaan menarik kesimpulan tentang jenis produk dan fitur apa yang dicari orang. Mereka memodifikasi produk mereka untuk memenuhi preferensi konsumen.

Tapi siapa lagi yang bisa melihat kumpulan data ini? Dan mengapa kita harus peduli?

Jika pencarian Web Anda sendiri ada pada topik yang tidak berbahaya, dan Anda tidak peduli siapa yang melihat pertanyaan Anda, pertimbangkan beberapa topik yang mungkin ditelusuri orang dan pikirkan mengapa mereka mungkin ingin menjaga privasi mereka: masalah kesehatan dan psikologis, kebangkrutan, perjudian yang tidak terkontrol , Konspirasi sayap kanan, konspirasi sayap kiri, alkoholisme, informasi anti aborsi, informasi pro-aborsi, erotika, obat-obatan terlarang. Apa saja konsekuensi yang mungkin bagi seseorang yang melakukan riset ekstensif di Web untuk sebuah novel suspens tentang teroris yang berencana meledakkan pabrik-pabrik kimia?

Pada tahun 2006, pemerintah federal mempresentasikan Google dengan panggilan pengadilan*\_* untuk dua bulan permintaan pencarian pengguna dan semua alamat Web† yang diindeks Google.‡ Google memprotes, membawa masalah ini ke perhatian publik. Meskipun panggilan pengadilan tidak meminta nama pengguna, gagasan pemerintah mendapatkan akses ke detail pencarian orang-orang yang ngeri pendukung privasi dan banyak orang yang menggunakan mesin telusur. Pendukung privasi dan Google menentang preseden akses pemerintah ke massa besar seperti itu. data. Pengadilan mengurangi cakupan panggilan pengadilan, menghapus kueri pengguna.

Beberapa bulan kemudian, rilis database besar permintaan pencarian di AOL menunjukkan bahwa pelanggaran privasi terjadi bahkan ketika perusahaan tidak mengaitkan pertanyaan dengan nama orang. Terhadap kebijakan perusahaan, seorang karyawan menempatkan data di situs web untukpencarian peneliti teknologi. Data ini mencakup lebih dari 20 juta kueri penelusuran oleh lebih

dari 650.000 orang dari periode tiga bulan. Data mengidentifikasi orang dengandikodekan nomor ID yang, bukan berdasarkan nama. Namun, tidak sulit untuk menyimpulkan identitas beberapa

orang, terutama mereka yang mencari nama atau alamat mereka sendiri. Suatu proses yang disebut *reidentifikasi* mengidentifikasi yang lain. Identifikasi ulang berarti mengidentifikasi individu darisekumpulan data anonim. Jurnalis dan kenalan mengidentifikasi orang-orang dalam komunitas kecilyang mencari berbagai topik tertentu, seperti mobil yang mereka miliki,olahraga yangtim mereka ikuti, masalah kesehatan mereka, dan hobi mereka. Setelah diidentifikasi, seseorangterkait dengan semua pencariannya yang lain. AOL dengan cepat menghapus data, tetapi jurnalis,Sebuah panggilan pengadilan adalah perintah pengadilan bagi seseorang untuk memberikan kesaksian atau menyediakan dokumen atau informasi lain untukpenyelidikan atau pengadilan. Kami menggunakan alamat termWeb secara informal untuk pengidentifikasi, atau alamat, atau URL halaman atau dokumen di theWeb(rangkaian karakter satu jenis dalam browser Web).Diperlukan data untuk menanggapi tantangan pengadilan terhadap Undang-Undang Perlindungan Anak Online (COPA), sebuah undang-undang yang dimaksudkan untukmelindungi anak-anak dari materi online “berbahaya bagi anak di bawah umur.” (Kami membahas COPA dalam Bagian 3.2.2.)

Peneliti, dan lainnya sudah menyalinnya. Beberapa membuat seluruh kumpulan data tersedia di Web lagi.

**Contoh : Smartphone**

Dengan begitu banyak aplikasi smartphone pintar, berguna, dan gratis yang tersedia, siapa yang berpikir dua kali untuk mengunduhnya? Para peneliti dan jurnalis mencermati perangkat lunak dan aplikasi ponsel pintar dan menemukan beberapa kejutan.

Beberapa ponsel Android dan iPhone mengirim data lokasi (pada dasarnya lokasi menara seluler terdekat) ke Google dan Apple, masing-masing. Perusahaan menggunakan data untuk membangun layanan berbasis lokasi yang dapat sangat berharga bagi publik dan bagi perusahaan. (Peneliti industri memperkirakan pasar untuk layanan lokasi berada dalam miliaran dolar.) Data lokasi seharusnya anonim, tetapi para peneliti menemukan, dalam beberapa kasus, bahwa itu termasuk ID telepon.

Kira-kira setengah aplikasi dalam satu tes mengirim nomor ID telepon atau lokasi ke perusahaan lain (selain yang menyediakan aplikasi). Beberapa orang mengirim informasi usia dan jenis kelamin kepada perusahaan periklanan. Aplikasi mengirim data tanpa sepengetahuan atau persetujuan pengguna. Berbagai aplikasi menyalin daftar kontak pengguna ke server jarak jauh. Ponsel Android dan iPhone memungkinkan aplikasi menyalin foto (dan, misalnya, mempostingnya di Internet) jika pengguna mengizinkan aplikasi untuk melakukan hal-hal tertentu yang tidak ada hubungannya dengan foto. (Google mengatakan kemampuan ini berasal dari ketika foto berada di kartu memori yang dapat dilepas dan dengan demikian kurang rentan.6 Ini adalah pengingat bahwa desainer harus secara teratur meninjau dan memutakhirkan keputusan desain keamanan.)

Sebuah bank besar mengumumkan bahwa aplikasi mobile banking gratisnya secara tidak sengaja menyimpan nomor rekening dan kode akses keamanan dalam file tersembunyi di telepon pengguna. Pembuat ponsel menemukan cacat pada ponselnya yang memungkinkan aplikasi mengakses alamat email dan mengirim data tanpa izin pemilik. Beberapa iPhone menyimpan data bulan, dalam file tersembunyi, tentang di mana ponsel itu dan kapan, bahkan jika pengguna telah mematikan layanan lokasi. Data dalam file seperti itu rentan terhadap kerugian, peretasan, dan penyalahgunaan. Jika Anda tidak tahu telepon menyimpan informasi, Anda tidak tahu untuk menghapusnya. Mengingat kerumitan perangkat lunak ponsel pintar, ada kemungkinan bahwa perusahaan-perusahaan tersebut secara jujur ​​tidak berniat untuk melakukan hal-hal ini.

Mengapa itu penting? Daftar kontak dan foto kami adalah milik kami; kita harus mengendalikan mereka. Pencuri dapat menggunakan informasi akun kami untuk merampok kami. Aplikasi menggunakan fitur pada ponsel yang menunjukkan lokasi ponsel, tingkat cahaya, pergerakan ponsel, keberadaan ponsel lain di dekatnya, dan sebagainya. Mengetahui di mana kita telah selama periode waktu tertentu (dikombinasikan dengan informasi lain dari telepon) dapat memberi tahu banyak tentang kegiatan kami dan

*\_* Anggota AOL menggugat perusahaan untuk merilis permintaan pencarian mereka, mengklaim pembebasan itu melanggar sekitar 10

undang-undang federal dan negara bagian .

† Berbagai perusahaan menyediakan pembaruan perangkat lunak untuk masalah ini.

1. File di ratusan ribu siswa, pelamar, fakultas, dan / atau alumni dari

Universitas California, Harvard, Georgia Tech, Kent State, dan beberapa universitas lain,

beberapa dengan nomor Jaminan Sosial dan tanggal lahir (dicuri oleh peretas) .

2. Nama, tanggal lahir, dan mungkin nomor kartu kredit dari 77 juta orang yang bermain video

game online menggunakan Sony PlayStation (dicuri oleh peretas). 24 juta akun

lainnya terpapar ketika peretas masuk ke layanan game PC Sony Online Entertainment.

3. Rekaman sekitar 40 juta pelanggan toko pakaian diskon TJX (TJ Maxx,

Lebih lanjut tentangTJX

insiden: Bagian 5.2.5

Marshalls, dan lain-lain), termasuk nomor kartu kredit dan debit dan beberapa

nomor SIM (dicuri oleh peretas).

4. Bank of America disk dengan informasi akun (hilang atau dicuri saat transit).

5. Riwayat kredit dan data pribadi lainnya untuk 163.000 orang (dibeli daribesar

perusahaan databaseoleh cincin penipuan yang menyamar sebagai bisnis yang sah).

6. Nama pasien, nomor Jaminan Sosial, alamat, tanggal lahir, dantagihan medis

informasiuntuk mungkin 400.000 pasien di rumah sakit (pada laptop yang dicuri darirumah sakit

mobil karyawan).

7. Lebih dari 1000 laptop Departemen Perdagangan, beberapa dengan data pribadi dariSensus

kuesioner. (Pencuri mencuri beberapa dari mobil karyawan Sensus sementara; yang lain,

karyawan hanya terus.)

8. Informasi kontak rahasia untuk lebih dari satu juta pencari kerja (dicuri dari

Monster.com oleh peretas menggunakan server di Ukraina).

**Gambar 2.1** Informasi pribadi yang hilang atau dicuri.

minat, serta dengan siapa kita kaitkan (dan apakah lampu menyala). Seperti yang kami sebutkan di Bagian 1.2.1, itu juga dapat menunjukkan di mana kita cenderung berada pada waktu tertentu di masa depan.

Beberapa masalah yang kami jelaskan di sini akan dibahas pada saat Anda membaca ini; Intinya adalah kita cenderung melihat risiko privasi dan pelanggaran serupa di setiap jenis gadget atau kemampuan baru.

**Data yang dicuri dan hilang**

Penjahat mencuri data pribadi dengan meretas ke sistem komputer, dengan mencuri komputer dan disk, dengan membeli atau meminta rekaman dengan alasan palsu, dan dengan menyuap karyawan Peretasan: Bagian 5.2 dari perusahaan yang menyimpan data. Broker informasi yang cerdik menjual data (termasuk catatan ponsel, laporan kredit, laporan kartu kredit, catatan medis dan pekerjaan, dan lokasi keluarga, serta informasi tentang rekening keuangan dan investasi) yang mereka peroleh secara ilegal atau dengan cara yang dipertanyakan. Penjahat, pengacara, detektif swasta, pasangan, mantan pasangan, dan agen penegak hukum adalah salah satu pembeli. Seorang detektif swasta dapat memperoleh beberapa informasi ini di masa lalu, tetapi tidak dengan mudah, murah, dan cepat.

Risiko lain adalah kecelakaan (kadang-kadang cukup ceroboh) kerugian. Bisnis, lembaga pemerintah, dan lembaga lain kehilangan komputer, disk, kartu memori, dan laptop yang berisi data pribadi yang sensitif (seperti nomor Jaminan Sosial dan nomor kartu kredit) pada ribuan atau jutaan orang, yang mengekspos orang-orang terhadap potensi penyalahgunaan informasi mereka dan berlama-lama. ketidakpastian. Mereka secara tidak sengaja mengizinkan file sensitif untuk menjadi publik di Web. Peneliti menemukan informasi medis, nomor Jaminan Sosial, dan informasi pribadi atau rahasia sensitif lainnya tentang ribuan orang dalam file di Web yang hanya memiliki status akses yang salah.

Situs web dari beberapa bisnis, organisasi, dan lembaga pemerintah yang membuat informasi akun tersedia di Web tidak cukup mengotentikasi orang yang mengakses informasi, memungkinkan akses penipu. Pencuri data sering mendapatkan informasi sensitif melalui telepon dengan berpura-pura menjadi orang yang catatannya mereka cari. Mereka memberikan beberapa informasi pribadi tentang target mereka untuk membuat permintaan mereka tampak sah. Itulah salah satu alasan mengapa penting untuk berhati-hati bahkan dengan data yang tidak terlalu sensitif dengan sendirinya.

Gambar 2.1 menunjukkan contoh kecil insiden informasi pribadi yang dicuri atau hilang (Privacy Rights Clearinghouse mendaftar ribuan insiden semacam itu di situs webnya). Dalam banyak insiden, tujuan para pencuri adalah mengumpulkan data untuk digunakan dalam pencurian identitas dan penipuan, kejahatan yang kita diskusikan secara rinci di Bab 5.

**Ringkasan risiko**

Contoh-contoh yang kami jelaskan mengilustrasikan banyak poin tentang data pribadi. Kami meringkas di sini:

* Apa pun yang kami lakukan di dunia maya dicatat, setidaknya sebentar, dan terhubung ke komputer atau telepon kami, dan mungkin nama kami.
* Dengan jumlah ruang penyimpanan yang sangat besar yang tersedia, perusahaan, organisasi, dan pemerintah menyimpan data dalam jumlah besar yang tidak akan pernah terbayangkan oleh siapa pun di masa lalu.
* Orang sering tidak menyadari pengumpulan informasi tentang mereka dan kegiatan mereka.
* Perangkat lunak sangat kompleks. Terkadang bisnis, organisasi, dan pengelola situs web bahkan tidak tahu apa perangkat lunak yang mereka gunakan untuk mengumpulkan dan menyimpan.
* Kebocoran terjadi. Adanya data menghadirkan risiko.
* Kumpulan banyak barang kecil informasi dapat memberikan gambaran yang cukup rinci tentang kehidupan seseorang.
* Hubungan langsung dengan nama seseorang tidak penting untuk mengorbankan privasi. Identifikasi ulang menjadi lebih mudah karena kuantitas informasi pribadi yang disimpan dan kekuatan alat pencarian dan analisis data.
* Jika informasi ada di situs web publik, orang-orang selain mereka yang dimaksudkan akan menemukannya. Ini tersedia untuk semua orang.
* Begitu informasi masuk ke Internet atau ke dalam basis data, tampaknya akan bertahan selamanya. Orang (dan perangkat lunak otomatis) dengan cepat membuat dan mendistribusikan salinan. Hampir tidak mungkin untuk mengeluarkan informasi yang dilepaskan dari sirkulasi.
* Sangat mungkin bahwa data yang dikumpulkan untuk satu tujuan (seperti membuat panggilan telepon atau menanggapi permintaan pencarian) akan menemukan penggunaan lain (seperti perencanaan bisnis, pelacakan, pemasaran, atau investigasi kriminal).
* Pemerintah terkadang meminta atau menuntut data pribadi yang sensitif yang dipegang oleh bisnis dan organisasi.
* Kita sering tidak dapat secara langsung melindungi informasi tentang diri kita sendiri. Kami bergantung pada bisnis dan organisasi yang mengelolanya untuk melindunginya dari pencuri, pengumpulan yang tidak disengaja, kebocoran, dan pengintaian pemerintah.

### 2.1.3 Terminologi dan Prinsip untuk Mengelola Data Pribadi

Kami menggunakan istilah *informasi pribadi* sering dalam bab ini. Dalam konteks masalah privasi, itu mencakup informasi apa pun yang berkaitan dengan, atau dapat dilacak ke, seorang individu. Istilah ini tidak hanya berlaku untuk apa yang mungkin kita anggap sebagai informasi sensitif, meskipun itu termasuk itu. Ini juga mencakup informasi yang terkait dengan "pegangan" seseorang, nama pengguna, nama panggilan online, nomor identifikasi, alamat email, atau nomor telepon. Tidak hanya mengacu pada teks. Ini meluas ke informasi apa pun, termasuk gambar, dari mana seseorang dapat mengidentifikasi individu yang hidup.

**Penjelasa Persetujuan dan pengumpulan informasi tak terlihat**

Prinsip pertama untuk perlakuan etis atas informasi pribadi adalah *informed consent* . Ada rentang luar biasa untuk jumlah privasi yang diinginkan oleh orang yang berbeda. Beberapa blog tentang perceraian atau penyakit mereka. Beberapa mencurahkan rincian dari hubungan romantis mereka di acara televisi atau ratusan jaringan sosial friends.Others menggunakan uang tunai untuk menghindari meninggalkan catatan pembelian mereka, mengenkripsi semua email mereka,*\_* dan marah ketika seseorang mengumpulkan informasi tentang mereka. Ketika sebuah bisnis atau organisasi memberi tahu orang-orang tentang pengumpulan datanya dan menggunakan kebijakan atau tentang data yang dikumpulkan oleh perangkat atau aplikasi tertentu, setiap orang dapat memutuskan, sesuai dengan nilai-nilainya sendiri, apakah atau tidak untuk berinteraksi dengan bisnis atau organisasi atau apakah akan menggunakan perangkat atau aplikasi. *Pengumpulan informasi tak terlihat* menggambarkan pengumpulan informasi pribadi tanpa sepengetahuan orang itu. Masalah etika yang penting adalah bahwa jika seseorang tidak mengetahui pengumpulan dan penggunaannya, dia tidak memiliki kesempatan untuk menyetujui atau menahan persetujuan. Kami memberikan

*\_* Mengenkripsi data berarti memasukkannya dalam bentuk kode sehingga orang lain tidak dapat membacanya.

beberapa contoh yang melibatkan ponsel cerdas dan aplikasinya di bagian sebelumnya. Berikut ini contoh dari konteks lain.

* Sebuah perusahaan menawarkan program gratis yang mengubah kursor browser Web menjadi karakter kartun. Jutaan orang menginstal program tersebut tetapi kemudian menemukan bahwa program tersebut mengirim kepada perusahaan laporan situs web yang dikunjungi penggunanya, bersama dengan nomor identifikasi pelanggan dalam perangkat lunak.
* "Perekam data acara" dalam mobil merekam kecepatan mengemudi, apakah pengemudi memakai sabuk pengaman, atau informasi lainnya.
* "Riwayat sniffers" adalah program yang mengumpulkan informasi tentang aktivitas online seseorang berdasarkan warna yang berbeda yang digunakan browser untuk menampilkan situs yang baru-baru ini dikunjungi.
* Perangkat lunak yang disebut *spyware*, sering diunduh dari situs web tanpa sepengetahuan pengguna, diam-diam mengumpulkan informasi tentang aktivitas dan data seseorang di komputernya dan kemudian mengirimkan informasi melalui Internet kepada orang atau perusahaan yang menanamkan spyware. Spyware dapat melacak penjelajahan Web seseorang untuk perusahaan periklanan atau mengumpulkan kata sandi dan nomor kartu kredit yang diketik oleh pengguna. (Beberapa dari aktivitas ini ilegal, tentu saja.)

Ketika komputer dan telepon kita berkomunikasi dengan situs web, mereka harus memberikan informasi tentang konfigurasinya (misalnya, browser Web yang digunakan). Untuk persentase komputer yang tinggi, ada cukup variasi dan detail dalam konfigurasi untuk membuat "sidik jari" untuk setiap komputer. Beberapa perusahaan menyediakan perangkat perangkat lunak fingerprinting untuk memerangi penipuan dan pencurian kekayaan intelektual dan untuk melacak aktivitas online orang-orang untuk menargetkan iklan. Baik pengumpulan informasi konfigurasi dan pembuatan profil aktivitas tidak terlihat. Perusahaan keuangan yang menggunakan sidik jari perangkat untuk keamanan akun pelanggan cenderung mengatakan demikian dalam kebijakan privasi. Kami cenderung tidak tahu ketika seseorang menggunakannya untuk membangun profil pemasaran.

Apakah suatu contoh pengumpulan data tertentu atau tidak merupakan pengumpulan informasi yang tidak terlihat

dapat bergantung pada tingkat kesadaran publik. Beberapa orang tahu tentang perekam data acara di mobil; kebanyakan tidak.10 Sebelum rilis data pencarian pengguna AOL yang dijelaskan dalam Bagian 2.1.2, pengumpulan data permintaan pencarian adalah contoh pengumpulan informasi yang tidak terlihat; atau masih banyak orang. Banyak bisnis dan organisasi memiliki pernyataan kebijakan atau perjanjian pelanggan yang memberi tahu pelanggan, anggota, dan pelanggan tentang kebijakan mereka dalam mengumpulkan dan menggunakan data pribadi, tetapi banyak orang tidak membacanya. Dan jika mereka membacanya, mereka lupa. Dengan demikian, dapat ada dampak privasi yang signifikan dari banyak sistem otomatis yang mengumpulkan informasi dengan cara yang tidak jelas, bahkan ketika orang telah diberitahu. Namun, ada perbedaan penting antara situasi di mana orang-orang diberitahu tetapi tidak sadar dan situasi di mana pengumpulan informasi benar-benar terselubung, seperti di spyware dan di beberapa aplikasi ponsel pintar yang kami jelaskan di Bagian 2.1.2.

**Cookies**

*Cookies* adalah file yang disimpan situs web di komputer pengunjung. Di dalam cookie, situs menyimpan dan kemudian menggunakan informasi tentang aktivitas pengunjung. Misalnya, situs ritel mungkin menyimpan informasi tentang produk yang kami lihat dan konten "keranjang belanja" virtual kami. Pada kunjungan berikutnya, situs mengambil informasi dari cookie. Cookie membantu perusahaan menyediakan layanan pelanggan yang dipersonalisasi dan menargetkan iklan untuk kepentingan setiap pengunjung. Mereka juga dapat melacak aktivitas kami di banyak situs dan menggabungkan informasi. Awalnya, cookie menjadi kontroversial karena gagasan bahwa situs web menyimpan file di komputer pengguna tanpa pengetahuan pengguna yang mengejutkan dan mengganggu orang. Hari ini, lebih banyak orang yang menyadari cookie dan menggunakan alat untuk mencegah atau menghapusnya. Sebagai tanggapan, beberapa perusahaan yang melacak aktivitas online mengembangkan "supercookies" yang lebih canggih yang membuat ulang cookie yang dihapus dan sulit ditemukan dan dihapus.

**Penggunaan sekunder, penggalian data, pencocokan, dan pembuatan profil**

*Pikiran-pikiran saya yang paling pribadi, tragedi pribadi saya, rahasia tentanglain*

*orang, hanyalah data transaksi, seperti tanda terima belanja.*

- Seorang wanita yang catatan psikologinya dibaca oleh firma asuransi.

*Penggunaan sekunder* adalah penggunaan informasi pribadi untuk suatu tujuan selain dari yang orang itu berikan. Contohnya termasuk penjualan informasi konsumen kepada pemasar atau bisnis lain, penggunaan informasi di berbagai database untuk menolak seseorang pekerjaan atau untuk menyesuaikan pitch politik, Internal Revenue Service mencari catatan registrasi kendaraan

untuk orang-orang yang memiliki mobil dan perahu mahal (untuk menemukan orang-orang dengan penghasilan tinggi), penggunaan pesan teks oleh polisi untuk mengadili seseorang atas kejahatan, dan penggunaan database pelanggan supermarket untuk menunjukkan pembelian alkohol oleh seorang pria yang menggugat toko karena dia terjatuh.

*Penambangan data* berarti mencari dan menganalisis kumpulan data untuk menemukan pola dan mengembangkan informasi atau pengetahuan baru. Penelitian menggunakan data jejaring sosial dan data ponsel cerdas yang kami jelaskan dalam Bagian 1.2.1 adalah contoh. *Mencocokkan* berarti menggabungkan dan membandingkan informasi dari database yang berbeda, sering menggunakan pengenal seperti nomor Jaminan Sosial seseorang atau alamat Internet komputer mereka untuk mencocokkan catatan. *Profiling* berarti menganalisis data untuk menentukan karakteristik orang yang paling mungkin terlibat dalam perilaku tertentu. Bisnis menggunakan teknik ini untuk menemukan kemungkinan pelanggan baru. Instansi pemerintah menggunakannya untuk mendeteksi penipuan, menegakkan undang-undang lain, dan menemukan teroris. Penambangan data, pencocokan komputer, dan profil adalah, dalam banyak kasus, contoh penggunaan informasi pribadi sekunder.

Kita akan melihat contoh penggunaan sekunder sepanjang bab ini. Salah satu isu kontroversial tentang informasi pribadi adalah tingkat kontrol yang harus dimiliki orang atas penggunaan sekunder informasi tentang mereka. Berbagai kegunaan yang diilustrasikan oleh beberapa contoh yang kami berikan di atas menunjukkan bahwa jawaban yang sangat berbeda sesuai untuk pengguna yang berbeda dan penggunaan yang berbeda.

Setelah memberi tahu orang-orang tentang informasi pribadi apa yang dikumpulkan oleh organisasi dan apa yang dilakukannya dengan informasi itu, kebijakan privasi paling sederhana dan paling diinginkan berikutnya adalah memberi orang kontrol atas penggunaan sekunder. Dua bentuk paling umum untuk memberikan pilihan seperti itu adalah *memilih* dan *memilih*. Di bawah kebijakan opt-out, seseorang harus memeriksa atau mengklik kotak pada kontrak, formulir keanggotaan, atau perjanjian atau menghubungi organisasi untuk meminta agar mereka tidak menggunakan informasi seseorang dengan cara tertentu. Jika orang tersebut tidak mengambil tindakan, anggapannya adalah bahwa organisasi dapat menggunakan informasi tersebut. Di bawah kebijakan opt-in, pengumpul informasi tidak dapat menggunakannya untuk penggunaan sekunder kecuali orang tersebut secara eksplisit memeriksa atau mengklik sebuah kotak atau menandatangani formulir memungkinkan penggunaan. (Berhati-hatilah untuk tidak membingungkan keduanya. Di bawah kebijakan opt-out, lebih banyak orang cenderung "masuk," dan di bawah kebijakan opt-in, lebih banyak orang cenderung "keluar," karena praduga default adalah kebalikan dari nama kebijakan.) Opsi menyisih sekarang sudah umum. Perusahaan dan organisasi yang bertanggung jawab dan ramah konsumen sering mengatur default sehingga mereka tidak membagikan informasi pribadi dan tidak mengirim email pemasaran kecuali orang tersebut secara eksplisit mengizinkannya - yaitu, mereka menggunakan kebijakan opt-in. Khususnya dalam situasi di mana pengungkapan informasi pribadi dapat memiliki konsekuensi negatif dan tidak jelas bagi pelanggan bahwa organisasi mungkin mengungkapkannya, kegagalan untuk tidak mengungkapkan tanpa izin eksplisit (yaitu, kebijakan opt-in) adalah kebijakan yang bertanggung jawab.

**Prinsip-prinsip informasi yang adil**

pendukung privasi telah mengembangkan berbagai rangkaian prinsip untuk perlindungan data pribadi. Mereka sering disebut Prinsip Informasi yang Adil atau Praktik Informasi yang Adil. Gambar 2.2 menyajikan daftar prinsip seperti itu. Informed consent dan pembatasan penggunaan sekunder muncul dalam prinsip pertama dan ketiga. Anda jarang akan melihat titik terakhir pada Gambar 2.2 termasuk di antara Prinsip-Prinsip Informasi yang Adil, tetapi saya menganggapnya penting. Beberapa perusahaan dan organisasi menyerahkan data pribadi kepada agen penegak hukum dan agen pemerintah saat diminta. Beberapa melakukannya hanya jika disajikan dengan

panggilan pengadilan atau perintah pengadilan lainnya. Beberapa tantangan panggilan dari pengadilan; beberapa tidak. Beberapa menginformasikan pelanggan atau anggota mereka ketika mereka memberikan data pribadi kepada pemerintah; beberapa tidak. Entitas yang memegang data memutuskan seberapa jauh untuk melindungi privasi anggotanya atau pelanggan. Individu yang datanya mungkin dibebaskan oleh entitas jarang menyadari permintaan pemerintah. Dengan demikian, entitas yang memegang data memiliki tanggung jawab kepada orang-orang itu. Merencanakan ke depan untuk berbagai kemungkinan skenario, mengembangkan kebijakan, dan mengumumkannya (dan mengikutinya) adalah bagian dari manajemen yang bertanggung jawab atas data pribadi orang lain.

1. Informasikan kepada orang-orang ketika Anda mengumpulkan informasi tentang mereka, apa yang Anda kumpulkan, dan bagaimana Anda

menggunakannya.

2. Kumpulkan hanya data yang dibutuhkan.

3. Tawarkan cara agar orang memilih keluar dari milis, iklan, dansekunder lainnya

penggunaan. Tawarkan cara agar orang-orang memilih keluar dari fitur dan layanan yang memaparkanpribadi

informasi.

4. Simpan data hanya selama diperlukan.

5. Menjaga keakuratan data. Jika sesuai dan masuk akal, berikan cara bagi orang

untuk mengakses dan perbaiki data yang disimpan tentang mereka.

6. Lindungi keamanan data (dari pencurian dan dari kebocoran tidak disengaja). Berikan perlindungan yang lebih kuat

untuk data sensitif.

7. Kembangkan kebijakan untuk menanggapi permintaan penegakan hukum untuk data.

**Gambar 2.2.** Prinsip-prinsip privasi untuk informasi pribadi.

Banyak bisnis dan organisasi telah mengadopsi beberapa versi Praktik Informasi Adil. Hukum di Amerika Serikat, Kanada, dan negara-negara Eropa (antara lain) mengharuskan mereka dalam banyak situasi. Prinsip-prinsip ini adalah pedoman etika yang masuk akal. Namun, ada variasi interpretasi prinsip yang luas. Misalnya, bisnis dan pendukung privasi tidak setuju tentang apa yang bisnis informasi "butuhkan" dan untuk berapa lama.

Mungkin sulit menerapkan prinsip-prinsip informasi yang adil ke beberapa teknologi dan aplikasi baru. Mereka tidak sepenuhnya mengatasi masalah privasi yang muncul dengan peningkatan kamera di tempat umum (seperti sistem kamera polisi dan Google Street View), sejumlah besar informasi pribadi yang dibagikan orang-orang di jejaring sosial, dan di mana-mana serta kekuatan ponsel cerdas. Misalnya, ketika seseorang memasukkan informasi pribadi dalam tweet ke ribuan orang, bagaimana cara menentukan tujuan yang dia berikan informasi? Bisakah penerima menggunakan informasi dengan cara apa pun? Seberapa luas penyebaran informasi yang harus ada sebelum publik dalam arti bahwa setiap orang dapat melihat atau menggunakannya? Bahkan ketika orang-orang setuju untuk berbagi informasi, konsekuensi cara-cara baru berbagi atau informasi baru dapat menjadi tidak terduga dan bermasalah. Misalnya, di Bagian 2.3.2 kami membahas pengaturan default untuk fitur di jejaring sosial yang memiliki konsekuensi signifikan.

## 2.2 Amandemen Keempat, Pengharapan Privasi, dan Teknologi Pengawasan

Dalam novel dystopian George Orwell *1984*, Big Brother (pemerintah) dapat menonton semua melalui "teleskrin" di semua rumah dan tempat umum. Ada sedikit kejahatan dan sedikit perbedaan pendapat politik — dan tidak ada cinta dan kebebasan. Saat ini, pemerintah tidak harus mengawasi setiap langkah yang kita buat, karena begitu banyak kegiatan kami meninggalkan jejak data dalam basis data yang tersedia bagi lembaga pemerintah.*\_* Ketika Big Brother ingin melihat langsung pada kami dan kegiatan kami, dia menggunakan alat-alat pengintai baru yang canggih. Pada bagian ini, kami mempertimbangkan dampak dari alat-alat ini pada privasi dan melihat kompatibilitasnya dengan perlindungan konstitusi dan hukum dari gangguan pemerintah.

### 2.2.1 Amandemen Keempat

*Hak rakyat untuk merasa aman dalam diri orang-orang, rumah, kertas,*

*dan efeknya, terhadap pencarian dan penyitaan yang tidak masuk akal, tidak*

*boleh dilanggar, dan tidak ada Waran yang akan dikeluarkan, tetapi atas kemungkinan penyebab, yang*

*didukung oleh Sumpah atau penegasan, dan khususnya menggambarkan*

*tempat yang akan dicari, dan orang-orang atau hal-hal yang akan disita.*

—Pembelian Empat, Konstitusi AS Konstitusi

AS melindungi hak privasi dari intrusi pemerintah, yang paling eksplisit dalam Amandemen Keempat. Mahkamah Agung AS telah menafsirkan bagian lain dari Bill of Rights untuk memberikan hak konstitusional untuk privasi dari pemerintah di daerah lain juga. Inggris memiliki tradisi yang sama, seperti yang diungkapkanberwarna-warniWilliam Pitt

dalam pernyataanpada 1763:

Orang termiskin mungkin di pondoknya menentang semua kekuatan Mahkota. Mungkin

lemah; atapnya bisa bergetar; angin bisa bertiup melaluinya; badai bisa masuk;

hujandapat masuk tapi Raja Inggris tidak bisa masuk.

Di sini, kami melihat bagaimana basis data, teknologi pengawasan, dan gadget konsumen populer mengancam hak ini. Meskipun pembahasan dalam bagian ini adalah dalam konteks Amandemen Keempat AS dan putusan Mahkamah Agung AS, risiko teknologi baru dari gangguan oleh pemerintah serupa di negara-negara lain.

Amandemen Keempat menetapkan batasan pada hak pemerintah untuk mencari rumah dan bisnis kita dan untuk menyita dokumen dan efek pribadi lainnya. Ini mengharuskan pemerintah memiliki kemungkinan penyebab untuk pencarian dan penyitaan. Artinya, harus ada bukti yang baik untuk mendukung pencarian spesifik. Dua masalah utama muncul dari teknologi baru. Pertama, banyak dari informasi pribadi kita tidak lagi aman di rumah kita atau di setiap kantor dokter dan penasihat keuangan kita. Kami membawa sejumlah besar informasi pribadi di ponsel pintar dan laptop. Banyak informasi pribadi ada dalam basis data besar di luar kendali kita. Banyak undang-undang mengizinkan lembaga penegak hukum untuk mendapatkan informasi dari basis data nonpemerintah tanpa perintah pengadilan. Aturan privasi federal memungkinkan lembaga penegak hukum mengakses catatan medis tanpa perintah pengadilan. The USA PATRIOT

*\_* Penggunaan segudang sistem data pribadi untuk menyelidiki atau memantau orang-orang kadang-kadang disebut *dataveillance*, kependekan

dari "pengawasan data."

Undang-Undang (disahkan setelah serangan teroris pada tahun 2001) mempermudah akses pemerintah ke berbagai jenis informasi pribadi, termasuk perpustakaan dan catatan keuangan, tanpa perintah pengadilan. Faktor kedua yang melemahkan perlindungan Amandemen Keempat adalah bahwa teknologi baru memungkinkan pemerintah untuk mencari rumah kita tanpa memasukkannya, untuk mencari orang-orang kita dari jarak jauh tanpa sepengetahuan kita, dan untuk mengekstrak semua data pada ponsel (termasuk data yang dihapus dan data yang dilindungi kata sandi ) dalam waktu kurang dari dua menit di perhentian lalu lintas.

Karena kami mempertimbangkan semua informasi pribadi yang tersedia untuk lembaga pemerintah sekarang, kami dapat merefleksikan kekhawatiran Hakim Agung William O. Douglas tentang potensi penyalahgunaan dari akses pemerintah hanya ke catatan rekening giro seseorang. Pada tahun 1974, dia berkata: Dalam arti seseorang didefinisikan oleh cek yang dia tulis. Dengan memeriksa mereka, agen mendapatkan untuk mengetahui dokter, pengacara, kreditor, sekutu politik, koneksi sosial, agama afiliasi, minat pendidikan, makalah dan majalah yang dia baca, dan seterusnya iklan infinitum. Semua ini terikat pada nomor jaminan sosial seseorang, dan sekarang kita memiliki

bank data, barang-barang lain ini akan memperkaya gudang itu dan memungkinkan bagi birokrat — dengan menekan satu tombol — untuk mendapatkan secara instan nama-nama dari 190 juta orang Amerika yang merupakan subversif atau calon potensial dan kemungkinan besar.15 Pembaca hari ini seharusnya tidak melewatkan ironi kalimat terakhir: 190 juta adalah hampir seluruh populasi Amerika Serikat pada saat itu. Dengan setiap penyimpanan data baru atau teknologi pencarian, lembaga penegak hukum dan sipil libertarian mempertanyakan pertanyaan apakah Amandemen Keempat berlaku. Di depan beberapa bagian, kami membahas teknologi tersebut dan beberapa prinsip yang dimiliki oleh Mahkamah Agung mapan.

*Ketika Republik Amerika didirikan, para perumus membangun*

*keseimbangan libertarian di antara nilai-nilai privasi,bersaing*

*pengungkapan, dan pengawasan yang. Keseimbangan ini didasarkan padateknologi*

*realitaskehidupan abad kedelapan belas. Karena penyiksaan dan inkuisisi adalah*

*satu-satunya cara yang diketahui untuk menembus pikiran, semua tindakan tersebut oleh*

*pemerintah dilarang oleh hukum. Entri fisik dan menguping*

*adalah satu-satunya cara menembus rumah pribadi dan ruang pertemuan;*

*Oleh karena itu para perumus membuat menguping oleh orang-orang pribadi kejahatan*

*dan memungkinkan pemerintah untuk memasuki tempat pribadi hanya untukmasuk akal*

*pencarian yang, di bawah kontrol surat perintah yang ketat. Karena prosedur pendaftaran*

*dan dokumen kepolisian adalah cara yang digunakan untuk mengontrol pergerakan bebas*

*orang-orang "kontroversial", praktik polisi Eropa ini dihalangi*

*oleh praktik pemerintah Amerika dan realitasseluler*

*kehidupan perbatasan.*

—Alan F. Westin,, *Privasidan Kebebasan*16

### 2.2.2 Teknologi Baru, Keputusan Mahkamah Agung, dan Ekspektasi Privasi

*Prinsip-prinsip yang ditetapkan dalam pendapat ini. . . berlaku untuk semua invasi*

*di pihak pemerintah dan karyawannya tentang kesucian rumah seorang lelaki*

*dan keistimewaan hidup. Itu bukan pemutusan pintunya,*

*dan penggeledahan di lacinya, yang merupakan esensi dari*

*pelanggaran itu; tetapi itu adalah invasi atas hak pribadinya yang tak terbatas*

*, kebebasan pribadi dan kepemilikan pribadi.*

—Justice Joseph Bradley,Noninvasive but deep disclaling *Boyd v. Amerika Serikat*, 1886.

**“Non invasiv tetapi sangat terbuka” Pencarian**

Judul di atas adalah dari deskripsi Julian Sanchez tentang berbagai teknologi pencarian dan pendeteksian.17 Banyak yang terdengar seperti fiksi ilmiah; mereka tidak. Teknologi ini dapat mencari rumah dan kendaraan kami tetapi tidak mengharuskan polisi untuk secara fisik masuk atau membukanya. Mereka dapat mencari tubuh kita di bawah pakaian kita dari kejauhan tanpa sepengetahuan kita. Batasan apa yang harus kita tempatkan pada penggunaannya? Kapan kita harus mengizinkan instansi pemerintah untuk menggunakannya tanpa surat perintah penggeledahan?

Alat-alat pencarian non-invasif tetapi sangat terbuka (beberapa digunakan dan sebagian dalam pengembangan) termasuk sniffer partikel yang mendeteksi banyak obat dan bahan peledak spesifik, sistem pencitraan yang mendeteksi senjata di bawah pakaian dari jarak jauh, perangkat yang menganalisis komposisi molekul kargo truk tanpa membuka truk , perangkat thermal-imaging (untuk menemukan lampu panas untuk menanam mariyuana, misalnya), dan perangkat yang menemukan seseorang dengan menempatkan ponselnya. Perangkat ini memiliki aplikasi keamanan dan penegakan hukum yang sangat berharga, tetapi teknologi ini dapat digunakan untuk pencarian acak, tanpa jaminan pencarian atau kemungkinan penyebabnya, pada orang yang tidak menaruh curiga. Seperti yang Sanchez tunjukkan, kita hidup “di negara yang rimnya peraturan membuat hampir semua orang bersalah atas beberapa pelanggaran pada titik tertentu.”18 Sebelum pemerintah mulai menggunakan alat ini, katakanlah, orang biasa yang membawa obat pulang dari Kanada, membuat sendiri bir, atau menyimpan pemanis terlarang atau lemak jenuh di rumah mereka (atau apa pun yang mungkin ilegal di masa depan), sangat penting untuk perlindungan privasi bahwa kita memiliki pedoman yang jelas untuk penggunaannya - dan, khususnya, klarifikasi kapan penggunaan tersebut merupakan pencarian yang membutuhkan surat perintah pencarian.

**Keputusan Mahkamah Agung dan harapan privasi**

Beberapa kasus Mahkamah Agung telah membahas dampak dari teknologi sebelumnya pada perlindungan Perubahan Keempat. Di *Olmstead v. Amerika Serikat*,19 tahun 1928, pemerintah telah menggunakan penyadapan telepon tanpa perintah pengadilan. Mahkamah Agung mengizinkan penyadapan. Ini menafsirkan Perubahan Keempat hanya berlaku untuk gangguan fisik dan hanya untuk pencarian atau penyitaan hal-hal materi, bukan percakapan. Hakim Louis Brandeis tidak sependapat, dengan alasan bahwa para penulis Perubahan Keempat melakukan semua yang mereka bisa untuk melindungi kebebasan dan privasi — termasuk privasi percakapan — dari gangguan oleh pemerintah berdasarkan teknologi yang tersedia pada saat itu. Dia percaya bahwa pengadilan harus menafsirkan Amandemen Keempat sebagai membutuhkan perintah pengadilan bahkan ketika teknologi baru memberikan pemerintah akses ke kertas dan percakapan pribadi kita tanpa memasuki rumah kita. Di *Katz v. Amerika Serikat*, pada tahun 1967, Mahkamah Agung membalikkan posisinya dan memutuskan bahwa Amandemen Keempat berlaku untuk percakapan dan itu berlaku di tempat umum dalam beberapa situasi. Dalam kasus ini, agen penegak hukum memasang alat pendengar dan perekam elektronik di luar bilik telepon untuk merekam percakapan tersangka. Pengadilan mengatakan bahwa Amandemen Keempat "melindungi orang, bukan tempat," dan bahwa apa yang orang "berusaha untuk melestarikan sebagai pribadi, bahkan di daerah yang dapat diakses oleh publik, mungkin secara konstitusional dilindungi." Untuk mengganggu di tempat-tempat di mana orang yang masuk akal memiliki ekspektasi privasi yang masuk akal, agen pemerintah membutuhkan perintah pengadilan.

Meskipun keputusan Mahkamah Agung di *Katz v. Amerika Serikat* memperkuat perlindungan Amandemen Keempat dalam beberapa hal, ada risiko signifikan dalam mengandalkan "harapan privasi" yang wajar untuk menentukan area di mana para penegak hukum membutuhkan perintah pengadilan. Pertimbangkan dua teknologi di kotak terdekat. Satu trek tindakan pribadi dalam pandangan publik; yang lain melacak orang di tempat-tempat pribadi. Ketika orang-orang yang terinformasi dengan baik mulai memahami kemampuan alat pengawasan modern, kita mungkin tidak lagi mengharapkan privasi dari pemerintah, dalam arti praktis. Apakah itu berarti kita tidak harus memilikinya? Mahkamah Agung mengakui masalah ini di *Smith* *v. Maryland* , di mana ia mencatat bahwa, jika penegakan hukum mengurangi harapan privasi yang sebenarnya dengan tindakan "asing untuk kebebasan Amandemen Keempat yang diakui," ini seharusnya *tidak* mengurangi perlindungan Amandemen Keempat kita. Namun, Pengadilan telah menafsirkan "harapan privasi" dengan cara yang sangat membatasi. Sebagai contoh, itu memutuskan bahwa jika kita berbagi informasi dengan bisnis seperti bank kita, maka kita tidak memiliki harapan privasi yang wajar untuk informasi itu (*Amerika Serikat v. Miller*, 1976). Agen penegak hukum tidak membutuhkan perintah pengadilan untuk mendapatkan informasi. Penafsiran ini tampak aneh. Kami mengharapkan privasi dari informasi keuangan yang kami berikan kepada bank atau lembaga keuangan lainnya. Kami mengharapkan kerahasiaan dalam banyak jenis informasi yang kami bagikan dengan beberapa, terkadang dipilih dengan cermat, yang lain. Kami membagikan aktivitas Web kami dengan ISP, situs web, dan perusahaan mesin pencari hanya dengan mengetik dan mengklik. Kami berbagi banyak jenis informasi pribadi di situs web tertentu di mana kami berharap situs ini menjadi pribadi. Apakah aman daritanpa jaminan

pencarian?

Di *Kyllo v. Amerika Serikat* (2001), Mahkamah Agung memutuskan bahwa polisi tidak dapat menggunakan perangkat pencitraan panas untuk mencari rumah dari luar tanpa surat perintah penggeledahan. Pengadilan menyatakan bahwa di mana "pemerintah menggunakan perangkat yang tidak digunakan untuk umum secara umum, untuk mengeksplorasi detail dari rumah yang sebelumnya tidak dapat diketahui tanpa gangguan fisik, pengawasan adalah 'pencarian.'" Alasan ini menunjukkan bahwa ketika suatu teknologi menjadi lebih banyak digunakan, pemerintah dapat menggunakannya untuk pengawasan tanpa surat perintah.

**Melacak mobil dan ponsel**

Agen penegak hukum melacak ribuan lokasi orang setiap tahun. Terkadang mereka memiliki perintah pengadilan untuk melakukannya, dan beberapa kali tidak. Apakah mereka membutuhkannya? Kami menggambarkan dua kasus kunci sebagai contoh. Pada 2012, Mahkamah Agung memutuskan *AS* *v. Jones*, kasus besar pertama dari pengawasan teknologi digital. Apakah Amandemen Keempat melarang polisi secara diam-diam memasang alat pelacak GPS ke kendaraan seseorang tanpa surat perintah penggeledahan? Polisi mengatakan tidak; mereka bisa mengamati mobil tersangka ketika bergerak di jalan-jalan umum. Mereka berpendapat perangkat GPS adalah alat yang menghemat tenaga kerja. Pengadilan tidak setuju. Ada dua argumen yang mendukung perlindungan Amandemen Keempat dalam kasus ini. Pertama, kendaraan adalah salah satu "efek" seseorang yang Amandemen Keempat secara eksplisit melindungi. Kedua, melacak lokasi seseorang selama sebulan, 24 jam sehari, seperti dalam kasus ini,

melampaui seseorang yang mengamati mobil lewat di depan umum; itu melanggar harapan privasi seseorang. Pengadilan setuju (dengan suara bulat) dengan argumen pertama. Polisi membutuhkan surat perintah penggeledahan untuk memasang alat pengintai

ke kendaraan pribadi. Para hakim mengakui bahwa harapan akan privasi merupakan masalah utama dalam melacak kasus-kasus di mana secara langsung melampirkan perangkat tidak diperlukan, tetapi mayoritas memilih untuk meninggalkan keputusan tentang itu untukmasa depan

kasus-kasus.∗20 Polisi memiliki satu argumen menentang ekspektasi privasi di *AS v. Jones*: kendaraan berkeliling di depan umum. Misalkan seseorang ada di rumah, di rumah teman atau kekasih, di dalam gereja atau fasilitas kesehatan, atau pribadi apa pun ruang. Lembaga penegak hukum menggunakan perangkat untuk cari seseorang dengan menemukan ponselnya,

bahkan ketika orang itu tidak aktif menggunakan telepon.† Polisi tidak perlu memasuki tempat pribadi atau secara fisik melampirkan sesuatu ke properti seseorang. Dengan demikian, harapan privasi adalah masalah utama di sini. Pihak penegak hukum berpendapat bahwa pelacakan ponsel (yang telah mereka gunakan lebih dari 1000 kali, menurut *Wall* *Jalan Jurnal* Investigasi) tidak memerlukan surat perintah penggeledahan karena orang yang menggunakan layanan ponsel tidak memiliki harapan privasi tentang data lokasi yang dipancarkan telepon ke menara seluler. Pandangan ini mungkin mengejutkan sebagian besar

pemilik ponsel. Mahkamah Agung belum mendengar kasus tentang teknologi ini.

\* Empat hakim menulis pendapat bahwa pelacakan juga melanggar harapan privasi.

 Perangkat ini berpura-pura menjadi menara sel. Agen

berkeliling dengan itu dan mendapatkan ponsel target untuk terhubung

ke beberapa lokasi. Mereka kemudian melakukan triangulasi di

telepon dari data yang dikumpulkan oleh perangkat.

Standar ini memungkinkan waktu bagi pasar, kesadaran publik, dan teknologi untuk dikembangkan guna memberikan perlindungan privasi terhadap teknologi baru. Apakah ini merupakan standar yang masuk akal — adaptasi hukum yang wajar terhadap teknologi baru? Atau haruskah pengadilan mengijinkan pencarian? Atau apakah pemerintah harus memenuhi persyaratan Amandemen Keempat untuk setiap pencarian di rumah di mana surat perintah diperlukan sebelum teknologi itu ada?

*Kami menggunakan teknologi baru ini tidak menandakan bahwa kami kurang tertarik*

*pada privasi. Gagasan pemerintah memantau keberadaan*

*kami, kebiasaan kami, kenalan kami, dan kepentingan kami masih membuat kami takut. Kita*

*sering tidak tahu apa yang terjadi sampai terlambat.*

—Judge Alex Kozinski21

### 2.2.3 Pencarian dan Penyitaan Komputer dan Telepon

*Privasi dalam asosiasi kelompok dapat. . . sangat penting untuk pelestarian*

*kebebasan berserikat, terutama di mana kelompok mendukungsetuju*

*keyakinan yang tidak.*

—The Supreme Court, yang berkuasa atas upaya negara bagian Alabama untuk

mendapatkan daftar keanggotaan National Association for Advancement

of Colored People (NAACP) pada tahun 1950.

Daftar keanggotaan NAACP tidak ada di komputer pada 1950-an. Tidak diragukan lagi sekarang. Kami mempertimbangkan beberapa masalah tentang bagaimana Amandemen Keempat berlaku untuk pencarian komputer, telepon, dan perangkat elektronik lainnya. Sejauh mana surat perintah penggeledahan meluas

saat mencari komputer? Kapan surat perintah pencarian dibutuhkan?

Amandemen Keempat mensyaratkan bahwa perintah penggeledahan bersifat spesifik tentang objek pencarian atau penyitaan. Pengadilan secara tradisional mengambil pandangan bahwa jika seorang petugas dengan surat perintah melihat bukti kejahatan lain dalam pandangan biasa, petugas dapat menangkapnya dan jaksa dapat menggunakannya. Tetapi jumlah informasi atau bukti yang mungkin terlihat jelas di rumah atau kantor kecil dibandingkan dengan apa yang ada di komputer. Komputer di bisnis akan memiliki informasi tentang sejumlah besar orang. Daftar anggota, catatan bisnis, catatan medis, dan banyak hal lainnya dapat berada di komputer yang sama dengan agen penegak hukum yang dapat mencari dengan perintah penggeledahan untuk barang-barang tertentu yang terbatas. Akses oleh agen penegak hukum untuk semua data di komputer atau perangkat dapat menjadi ancaman serius terhadap privasi, kebebasan, dan kebebasan berbicara.

Bagaimana seharusnya kita menafsirkan "tampilan biasa" untuk pencarian file komputer atau ponsel cerdas? Interpretasi luas — misalnya, “semua file yang tidak dienkripsi” —menggunakan pelecehan. Agen bisa mendapatkan surat perintah untuk kejahatan kecil yang mereka punya bukti pendukung, dan kemudian pergi ke ekspedisi memancing untuk informasi lain. Ini menghalangi persyaratan Amandemen Keempat bahwa surat perintah harus spesifik. Dalam satu kasus, ketika mencari komputer seorang pria dengan surat perintah penggeledahan untuk bukti kejahatan narkoba, seorang petugas melihat nama file yang menunjukkan konten ilegal yang tidak terkait dengan surat perintah. Dia membuka file dan menemukan pornografi anak. Pengadilan banding mengatakan nama-nama file mungkin dianggap dalam tampilan biasa, tetapi

isi dari file tidak.23 Meskipun kejahatan dalam kasus ini sangat tidak menyenangkan, prinsip melindungi kita dari pelanggaran oleh polisi.

Dalam penyelidikan penggunaan obat peningkat kinerja oleh pemain bisbol profesional, agen penegak hukum memperoleh surat perintah penggeledahan untuk file komputer catatan laboratorium pada tes narkoba untuk 10 pemain khusus. File laboratorium yang mereka sita berisi catatan tentang ratusan pemain bisbol, pemain hoki, dan orang biasa yang bukan atlet. Para agen menemukan bahwa lebih dari 100 pemain baseball dinyatakan positif menggunakan steroid. Kasus ini mendapat banyak perhatian dalam pemberitaan ketika nama-nama pemain terkemuka yang diduga dites positif dibocorkan ke media berita. Pengadilan banding federal memutuskan bahwa informasi tentang semua kecuali 10 pemain asli berada di luar lingkup surat perintah penggeledahan dan pemerintah salah untuk mengambilnya.

Misalkan agen penegak hukum memiliki surat perintah penggeledahan untuk komputer tetapi menemukan bahwa file tersebut dienkripsi. Apakah pemiliknya menyediakan kunci enkripsi? Amandemen Kelima Konstitusi AS menetapkan bahwa seseorang tidak dapat dipaksa untuk bersaksi melawan dirinya sendiri. Namun, pengadilan terkadang memungkinkan pemerintah untuk meminta seseorang memberikan kunci atau kombinasi ke brankas. Aturan di pengadilan federal tidak konsisten tentang apakah persyaratan tersebut dapat diterapkan pada kunci enkripsi. (Dalam banyak kasus, agen penegak hukum mendekripsi file dengan cara lain.)

*Apa yang terjadi pada Amandemen Keempat?*

*Apakah itu dicabut entah bagaimana?*

- Seorang hakim, mengomentari perampasan catatan laboratorium untuk tes narkoba.

**Ponsel dan laptop**

Telepon seluler mungkin berisi kontak, nomor untuk panggilan yang dibuat dan diterima, email, pesan teks, dokumen, kalender pribadi, foto, riwayat penelusuran Web, dan catatan di mana telepon berada. Bagi banyak orang, telepon adalah kantor perjalanan, yang berisi informasi rahasia dan hak milik. Telepon seorang pengacara mungkin berisi informasi tentang klien dan kasus — secara hukum dilindungi dari akses oleh polisi.

Polisi dapat mencari orang yang ditangkap (tanpa surat perintah penggeledahan) dan memeriksa properti pribadi pada orang tersebut (dalam saku, misalnya) atau dalam jangkauannya. Apakah surat perintah pencarian diperlukan sebelum polisi dapat mencari isi ponsel orang tersebut? *Haruskah* surat perintah pencarian diperlukan?

Ini tampak seperti "no-brainer" klasik. Pengumpulan informasi yang luas tentang ponsel adalah jenis informasi yang dimaksudkan untuk dilindungi oleh Amandemen Keempat. Seorang hakim yang berkuasa terhadap pencarian ponsel mengatakan pembenaran untuk mengizinkan polisi untuk mencari orang yang ditangkap adalah untuk menemukan dan mengambil senjata dan untuk mencegah orang dari menyembunyikan atau menghancurkan bukti. Setelah polisi memiliki tahanan telepon, itu aman dari kehancuran dan polisi harus menunggu sampai mereka memiliki surat perintah pencarian sebelum mengambil informasi dari telepon. Mahkamah Agung Ohio memutuskan bahwa mencari telepon orang yang ditangkap tanpa surat perintah penggeledahan adalah inkonstitusional:*\_* orang memiliki harapan privasi untuk isi telepon mereka.

Namun Mahkamah Agung California memutuskan sebaliknya. Dikatakan bahwa pencarian isi ponsel diizinkan karena telepon itu milik pribadi ditemukan pada orang yang ditangkap. Polisi telah mencari ponsel yang diambil dari orang yang ditangkap dalam lusinan kasus tanpa surat perintah. Akhirnya, sebuah kasus yang mengangkat masalah ini akan didengar oleh Mahkamah Agung AS. Hasilnya akan memiliki implikasi mendalam untuk privasi. Sementara itu, pengacara menyarankan meninggalkan ponsel di luar jangkauan saat mengemudi.

Petugas bea cukai dan perbatasan mencari barang ketika warga AS kembali dari negara lain dan ketika orang asing memasuki Amerika Serikat. Petugas perbatasan mencari, dan kadang-kadang menyita, laptop dan telepon wartawan, pebisnis, dan wisatawan lainnya. Apakah mencari laptop setara dengan mencari koper? Atau, karena jumlah dan jenis informasi pribadi yang dikandungnya, apakah mencari mereka di perbatasan memerlukan kecurigaan yang wajar atas kejahatan? Pengadilan banding federal memutuskan bahwa agen bea cukai tidak perlu kecurigaan yang wajar atas kejahatan untuk mencari laptop, telepon, dan perangkat elektronik lainnya. Tuntutan hukum dan perdebatan tentang masalah ini sedang berlangsung.

### 2.2.4 Pengawasan Video dan Pengenalan Wajah

Kami terbiasa dengan kamera keamanan di bank dan toserba. Mereka membantu dalam penyelidikan kejahatan. Penjara menggunakan sistem pengawasan video untuk keamanan. Kasino judi menggunakannya untuk menonton para penipu yang dikenal. Sistem pengawasan video memonitor lalu lintas dan menangkap pengemudi yang menjalankan lampu merah. Dalam kasus ini, orang umumnya sadar akan pengawasan. Setelah serangan teroris tahun 2001, polisi di Washington, DC, memasang kamera yang memperbesar individu yang berjarak setengah mil.

Kamera saja meningkatkan beberapa masalah privasi. Ketika dikombinasikan dengan sistem pengenalan wajah, mereka meningkatkan bahkan lebih. Berikut adalah beberapa aplikasi kamera dan pengenalan wajah dan beberapa masalah privasi dan kebebasan sipil yang relevan.

Dalam aplikasi publik pengenalan wajah skala besar pertama, polisi inTampa, Florida, memindai wajah dari semua 100.000 penggemar dan karyawan yang memasuki Super Bowl 2001 (menyebabkan beberapa wartawan menjuluki Snooper Bowl). Sistem mencari file-file komputer penjahat untuk pertandingan, memberikan hasil dalam hitungan detik. Orang-orang tidak diberitahu bahwa wajah mereka dipindai. Tampa memasang sistem serupa di lingkungan restoran populer dan klub malam. Polisi di ruang kontrol diperbesar pada masing-masing wajah dan memeriksa kecocokan dalam database tersangka mereka.28 Dalam dua tahun penggunaan, sistem tidak mengenali siapa pun yang diinginkan polisi, tetapi kadang-kadang mengidentifikasi orang yang tidak bersalah sebagai penjahat yang dicari.

**\_ Pengadilan mengizinkan pengecualian dalam beberapa jenis keadaan darurat tertentu.**

ACLU membandingkan penggunaan sistem pengenalan wajah di Super Bowl dengan jajaran kepolisian yang terkomputerisasi di mana orang-orang yang tidak bersalah menjadi subjek tanpa sepengetahuan atau persetujuan mereka. Sistem pengenalan wajah memiliki tingkat akurasi yang buruk pada awal tahun 2000,29 tetapi teknologi meningkat, seiring dengan ketersediaan foto untuk dicocokkan (foto yang ditandai di jejaring sosial, misalnya). Seorang petugas polisi sekarang dapat mengambil foto seseorang di jalan dan menjalankan aplikasi ponsel untuk pengenalan wajah. (lain

Aplikasimemindai iris seseorang dan mengumpulkan sidik jari.)

Beberapa kota telah meningkatkan program pengawasan kamera mereka, sementara yang lain menyerahkan sistem mereka karena mereka tidak secara signifikan mengurangi kejahatan. (Beberapa mendukung pencahayaan yang lebih baik dan lebih banyak patroli polisi - teknologi rendah dan kurang invasif dari privasi.) Para pejabat kota Toronto menolak untuk membiarkan polisi mengambil alih kamera lalu lintas mereka untuk memantau pawai protes dan mengidentifikasi organisasinya. Dalam pernyataan kontroversial, Komisaris Privasi Kanada berpendapat bahwa Privacy Act di negara itu membutuhkan “kebutuhan yang dibuktikan untuk setiap bagian informasi pribadi yang dikumpulkan” untuk melaksanakan program pemerintah dan oleh karena itu merekam aktivitas sejumlah besar masyarakat umum bukanlah cara yang diperbolehkan. pencegahan kejahatan.30

Inggris adalah negara pertama yang mendirikan sejumlah besar kamera di tempat umum untuk mencegah kejahatan. Ada jutaan kamera pengintai di Inggris. Sebuah penelitian oleh sebuah universitas di Inggris menemukan sejumlah pelanggaran oleh operator kamera pengintai, termasuk mengumpulkan rekaman yang bernada hina, seperti orang-orang yang berhubungan seks di dalam mobil, dan menunjukkannya kepada rekan-rekannya. Pengacara pembela mengeluh bahwa jaksa kadang-kadang merusak rekaman yang dapat mengungkap

tersangka.31 Menegakkan jam malam bagi kaum muda adalah salah satu penggunaan kamera publik di Inggris. Aplikasi ini menunjukkan jenis pemantauan dan kontrol dari populasi khusus yang membuat kamera menjadi mudah. Apakah polisi akan menggunakan sistem pengenalan wajah untuk melacak para pembangkang politik, jurnalis, lawan-lawan politik dari orang-orang berkuasa — jenis-jenis orang yang ditargetkan untuk pengawasan ilegal atau diragukan di masa lalu? Pada tahun 2005, pemerintah Inggris merilis laporan yang mengatakan sistem TV sirkuit tertutup Inggris tidak banyak

digunakan dalam memerangi kejahatan. Satu-satunya penggunaan kamera yang berhasil adalah di tempat parkir di mana mereka membantu mengurangi kejahatan kendaraan.32 Belakangan tahun itu, foto-foto yang diambil oleh kamera pengintai membantu mengidentifikasi teroris yang memicu bom di kereta bawah tanah London. Setelah perusuh membakar dan menjarah lingkungan di Inggris pada tahun 2011, polisi menggunakan rekaman dari kamera jalanan dan sistem pengenalan wajah untuk mengidentifikasi para perusuh. Sangat jarang untuk semua fakta atau argumen kuat untuk mendukung hanya satu sisi dari suatu masalah. Apa untung-rugi antara privasi dan mengidentifikasi penjahat dan teroris yang mau kita buat?

Departemen Transportasi California memotret pelat nomor mobil yang mengendarai mobil di area tertentu. Kemudian menghubungi pemilik mobil untuk survei tentang lalu lintas di daerah tersebut. Ratusan pengemudi mengeluh. Orang-orang ini keberatan dengan apa yang mereka anggap sebagai pengawasan yang tidak dapat diterima oleh lembaga pemerintah bahkan ketika agensi hanya memotret pelat nomor mereka, bukan wajah mereka — untuk survei, bukan tindakan polisi. Banyak orang biasa tidak suka dilacak dan difoto tanpa sepengetahuan mereka.

Jelas, beberapa aplikasi kamera dan sistem pengenalan wajah adalah penggunaan teknologi yang wajar dan bermanfaat untuk keamanan dan pencegahan kejahatan. Tetapi ada kebutuhan yang jelas untuk batasan, kontrol, dan pedoman. Bagaimana seharusnya kita membedakan yang tepat dari penggunaan yang tidak pantas? Haruskah acara internasional seperti Olimpiade, yang terkadang target teroris, menggunakan sistem seperti itu? Haruskah kita membatasi teknologi seperti sistem pengenalan wajah untuk menangkap teroris dan tersangka dalam kejahatan serius, atau haruskah kita mengizinkan mereka di tempat umum untuk menyaring orang-orang dengan tiket parkir yang belum dibayar? Apakah orang memiliki hak untuk mengetahui kapan dan di mana kamera digunakan? Di Amerika Serikat, polisi harus memiliki alasan untuk mewajibkan seseorang untuk diambil sidik jarinya. Haruskah standar yang sama berlaku untuk penggunaan pengenalan wajah dan pemindaian iris? Jika kami menganggap masalah ini cukup dini, kami dapat mendesain fitur perlindungan privasi ke dalam teknologi, menetapkan kebijakan yang dipikirkan matang untuk penggunaannya, dan mengeluarkan undang-undang perlindungan privasi yang sesuai sebelumnya, karena Mahkamah Agung Kanada khawatir dengan kutipan di bawah ini , "Privasi dimusnahkan."

*Untuk mengizinkan pengawasan video yang tidak terbatas oleh agen negara akan*

*sangat mengurangi tingkat privasi yang dapat kita harapkan*

*untuk dinikmati dalam masyarakat yang bebas. . . . Kita harus selalu waspada terhadap fakta*

*bahwa metode modern pengawasan elektronik memiliki potensi, jika*

*tidak terkendali, untuk menghilangkan privasi.*

—Supreme Court of Canada.

*Ini adalah pertemuan publik!*

—Reporter Pete Tucker, atas penangkapannya karena mengambil foto dengan

telepon genggamnya di sebuah pertemuan terbuka dari sebuah lembaga pemerintah AS. Wartawan

Jim Epstein kemudian ditangkap karena merekam penangkapan Tucker di

teleponnya sendiri.

## 2.3 Sektor Bisnis dan Sosial

### 2.3.1 Pemasaran dan Personalisasi

*Acxiom memberikan gambaran yang lengkap dan akurat tentang pelanggan dan*

*prospek, memperkuat semua upaya pemasaran dan hubungan.*

—Situs situs web

Pemasaran adalah tugas penting bagi sebagian besar bisnis dan organisasi. Ini adalah salah satu penggunaan terbesar informasi pribadi — oleh bisnis, partai politik, organisasi nonprofit, dan kelompok advokasi. Pemasaran termasuk mencari pelanggan baru, anggota, atau pemilih.



**Penambangan data dan pemasaran yang cerdik.**

Pelanggan perusahaan ritel Inggris Tesco mengizinkan perusahaan untuk mengumpulkan informasi tentang kebiasaan pembelian mereka dengan imbalan diskon. Perusahaan mengidentifikasi laki-laki dewasa muda yang membeli popok dan mengirim mereka kupon untuk bir. Dengan asumsi bahwa, dengan bayi baru, mereka memiliki lebih sedikit waktu untuk pergi ke pub. Target mengalahkan itu. Penambang data Target menganalisis pembelian wanita yang mendaftar untuk registrasi bayi. Mereka menemukan bahwa wanita hamil cenderung meningkatkan pembelian mereka dari sekelompok 25 produk. Jadi, jika seorang wanita mulai membeli lebih banyak dari beberapa produk tersebut (misalnya, losion yang tidak beraroma dan suplemen mineral), Target mulai mengirim kupon dan iklan untuk kehamilan dan produk bayi. Ia bahkan dapat mengatur waktu mereka untuk tahap-tahap kehamilan. Untuk bersaing dengan Wal-Mart, Tesco bertujuan untuk mengidentifikasi pelanggan yang paling sadar harga dan karenanya kemungkinan besar tertarik

pada harga rendah Wal-Mart. Dengan menganalisis data pembelian, perusahaan menentukan pelanggan mana yang secara teratur membeli versi produk termurah yang tersedia di lebih dari satu tingkat harga. Kemudian mereka menentukan produk apa yang paling sering dibeli oleh pelanggan, dan mereka menetapkan harga untuk produk-produk tersebut di bawah Mart-Mart. Apakah ini contoh persaingan yang diinginkan atau campur tangan dan manipulasi yang menakutkan dari konsumen?

dan mendorong yang lama untuk melanjutkan. Ini termasuk mengiklankan produk, layanan, atau penyebab seseorang. Ini termasuk bagaimana harga produk dan kapan dan kepada siapa untuk menawarkan diskon.

Melalui sebagian besar abad ke-20, bisnis mengirimkan katalog dan iklan berdasarkan beberapa kriteria (usia, jenis kelamin, dan lingkungan, misalnya). Komputer dan peningkatan kapasitas penyimpanan pada 1980-an dan 1990-an memulai revolusi dalam pemasaran bertarget. Sekarang, bisnis menyimpan dan menganalisis data dalam jumlah terabyte, termasuk pembelian konsumen, informasi keuangan, aktivitas online, opini, preferensi, catatan pemerintah, dan informasi berguna lainnya untuk menentukan siapa yang mungkin menjadi pelanggan baru dan apa produk dan layanan baru yang mungkin pelanggan lama membeli. Mereka menganalisis ribuan kriteria untuk menargetkan iklan baik online maupun offline. Pengecer online membuat rekomendasi kepada Anda berdasarkan pembelian Anda sebelumnya dan orang-orang dari orang lain dengan pola pembelian yang sama. Situs web menyambut kami dengan nama dan memberi kami opsi berdasarkan aktivitas sebelumnya di situs itu.

Bagi banyak orang, gagasan bahwa pedagang mengumpulkan, menyimpan, dan menjual data tentang kebiasaan pembelian mereka sangat mengganggu. Kegiatan-kegiatan ini mempengaruhi aspek kunci privasi: pengendalian informasi tentang diri sendiri. Pendukung privasi dan beberapa konsumen keberatan dengan iklan berdasarkan riwayat pembelian konsumen dan aktivitas online. Pemasar berargumentasi bahwa pemasaran yang ditargetkan dengan baik berguna bagi konsumen dan mengurangi biaya overhead dan, pada akhirnya, biaya produk. LL Bean, sebuah bisnis mail-order yang besar, mengatakan bahwa mereka mengirimkan lebih sedikit katalog karena lebih baik dalam menargetkan pelanggan. Sebuah perusahaan iklan Web mengatakan pengguna mengklik 16% dari iklan yang ditampilkan berdasarkan profil aktivitas pengguna — lebih banyak daripada 1% khas

untuk iklan Web yang tidak bertarget. Perusahaan lain mengatakan bahwa 20-50% orang menggunakan kupon pribadi yang disediakan di layar atau melalui email, dibandingkan dengan tingkat penebusan 1-5% untuk sisipan surat kabar. Perusahaan-perusahaan mengatakan menargetkan iklan melalui informasi konsumen pribadi mengurangi jumlah iklan secara keseluruhan yang orang akan lihat dan menyediakan iklan yang kemungkinan besar orang inginkan.37 Banyak orang menyukai personalisasi iklan dan rekomendasi. Penargetan sangat populer di kalangan orang-orang yang diiklankan Google bahwa Gmail tidak menampilkan *bertarget* iklan spanduk yang tidak.

Beberapa jenis personalisasi yang kurang jelas mengganggu orang lebih banyak (ketika mereka belajar dari mereka). Tampilan, iklan, harga, dan diskon yang Anda lihat saat berbelanja online mungkin berbeda dari yang dilihat orang lain. Beberapa penargetan semacam itu cukup beralasan: Sebuah situs pakaian tidak menampilkan parka musim dingin di halaman beranda untuk pembelanja dari Florida. Beberapa situs menawarkan diskon kepada pengunjung pertama kali. Beberapa menampilkan ratusan variasi halaman tergantung pada waktu, jenis kelamin, lokasi, dan lusinan atribut lain dari sesi seseorang. (Beberapa situs menebak jenis kelamin pengunjung berdasarkan perilaku mengklik.38) Jika seseorang ragu-ragu terhadap suatu produk, sebuah situs mungkin menawarkan sesuatu yang ekstra, mungkin pengiriman gratis. Apakah pengumpulan dan penggunaan informasi perilaku ini merupakan contoh pengumpulan informasi tak terlihat yang tidak pantas? Ketika kami berbelanja di toko, pegawai penjualan dapat melihat jenis kelamin dan perkiraan usia kami. Mereka dapat membentuk kesimpulan lain tentang kita dari pakaian, percakapan, dan perilaku kita. Penjual yang baik di toko-toko khusus yang mahal, dealer mobil, pasar loak, dan pasar jalanan dunia ketiga membuat penilaian tentang berapa banyak pelanggan potensial akan membayar. Mereka memodifikasi harga atau menawarkan ekstra sesuai. Apakah perangkat lunak kompleks yang mempersonalisasi belanja online hanya mengimbangi hilangnya informasi yang akan tersedia bagi penjual jika kita berbelanja secara langsung? Apakah sebagian orang gelisah karena mereka tidak menyadari bahwa perilaku mereka memengaruhi apa yang muncul di layar mereka? Apakah orang gelisah karena mereka tidak menyadari bahwa situs web dapat menentukan (dan menyimpan) banyak hal tentang mereka ketika mereka berpikir mereka menjelajah secara anonim? Apakah kegelisahan itu akan kita atasi karena kita memahami teknologi dengan lebih baik? Atau apakah ada ancaman privasi yang bersembunyi di praktik-praktik ini?

Perusahaan dapat menggunakan sistem pengenalan wajah di konsol gim dan televisi untuk menargetkan iklan kepada individu yang bermain game atau menonton TV. Risiko apa yang ditimbulkan oleh privasi ini? Apakah tidak etis untuk menyertakan fitur-fitur seperti itu? Apakah kebanyakan orang akan menyukai penyesuaian? Apakah mereka mengerti bahwa jika mereka melihat iklan yang ditargetkan untuk kepentingan mereka, seseorang di suatu tempat menyimpan informasi tentang mereka?

Contoh-contoh kami sejauh ini adalah situasi komersial. Partai Demokrat dan Republik menggunakan basis data yang luas pada puluhan juta orang untuk profil mereka yang mungkin memilih kandidat mereka. Pihak-pihak menentukan masalah apa yang harus ditekankan (dan yang harus dihilangkan) di bidang promosi yang dipersonalisasi. Basis data termasuk ratusan rincian seperti pekerjaan, hobi, jenis mobil, dan keanggotaan serikat.39 Satu pihak dapat mengirim selebaran kampanye kepada anggota serikat yang konservatif yang menekankan kebijakan ketenagakerjaannya tetapi tidak menyebutkan, katakanlah, aborsi, sementara pihak lain mungkin melakukan yang sebaliknya.

**Masalahnya adalah penjelasan dan persetujuan**

Perubahan teknologi dan sosial membuat orang tidak nyaman, tetapi itu tidak berarti perubahan itu tidak etis. Beberapa pendukung privasi ingin melarang semua iklan yang ditargetkan oleh perilaku online. Harus jelas bahwa pemasaran yang ditargetkan atau dipersonalisasi tidak, dengan sendirinya, tidak etis. Sebagian besar kekhawatiran yang sah berkaitan dengan bagaimana pemasar mendapatkan data yang mereka gunakan. Dalam beberapa kasus ada persetujuan, di beberapa tidak ada, dan dalam banyak kompleksitas situasi membuat persetujuan tidak jelas.

Pengumpulan data konsumen untuk pemasaran tanpa memberi tahu orang atau memperoleh persetujuan mereka tersebar luas, pada dasarnya praktik standar, sampai kira-kira akhir 1990-an. Kadang-kadang, konsumen kecil mencetak informasi, tetapi sering kali mereka tidak melihatnya, tidak memahami implikasinya, atau mengabaikannya. Secara bertahap, kesadaran publik dan tekanan untuk peningkatan meningkat, dan kebijakan pengumpulan dan distribusi data meningkat. Sekarang situs web, bisnis, dan organisasi umumnya menyediakan pernyataan multi-halaman eksplisit tentang informasi apa yang mereka kumpulkan dan bagaimana mereka menggunakan informasi tersebut. Mereka menyediakan opsi optout dan opt-in. (Undang-undang dan peraturan federal memerlukan perlindungan privasi khusus untuk informasi keuangan dan medis.40) Masih banyak perusahaan yang salah melakukannya, entah karena kurangnya perhatian untuk privasi orang atau dengan salah menilai apa yang diinginkan orang. Ada juga dunia pengumpulan data yang luas di mana kita memiliki sedikit atau tidak ada kontrol langsung. Ketika seseorang menyetujui penggunaan informasi konsumen oleh perusahaannya, orang tersebut mungkin tidak tahu seberapa luas perusahaan itu dan sejauh mana data itu dapat bepergian. Perusahaan seperti Acxiom (dikutip pada awal bagian ini), database internasional besar dan perusahaan direct-marketing, mengumpulkan data pribadi dari sejumlah besar sumber online dan offline. Perusahaan-perusahaan yang memelihara database konsumen besar membeli (atau bergabung dengan) orang lain, menggabungkan data untuk membangun basis data dan dokumen yang lebih rinci. Mereka menjual data dan profil konsumen ke bisnis untuk pemasaran dan "manajemen pelanggan." Kebanyakan orang tidak tahu perusahaan seperti itu ada.

Pelacakan ekstensif dan tersembunyi dari aktivitas online menyebabkan panggilan untuk tombol "Jangan Lacak" di browser. Arti dan efek yang tepat dari tombol tersebut belum ditentukan. Idenya adalah bahwa pengguna akan memiliki satu tempat yang jelas untuk menunjukkan bahwa mereka tidak ingin aktivitas Web mereka dilacak dan disimpan. Banyak pengiklan, penyedia browser Web populer, dan perusahaan Internet besar sepakat untuk menerapkan dan mematuhi beberapa versi Do Not Track.

Kesadaran bervariasi di antara konsumen, dan banyak yang tidak membaca kebijakan privasi. Apakah itu tanggung jawab pengguna untuk mengetahui pengumpulan data dan kebijakan pelacakan dari situs yang dia kunjungi? Apakah keputusan seseorang untuk berinteraksi dengan bisnis atau situs web merupakan persetujuan implisit terhadap pengumpulan data yang diposkan, pemasaran, dan kebijakan pelacakannya? Seberapa jelas, jelas, dan spesifik kebijakan penggunaan informasi? Seberapa seringkah situs yang menjalankan (atau mengizinkan pihak ketiga untuk menjalankan) perangkat lunak pelacakan mengingatkan pengguna? Beberapa orang yang mengizinkan pelacakan ekstensif dan pengumpulan informasi mungkin kemudian menyesali keputusan khusus yang mereka buat. Siapa yang bertanggung jawab untuk melindungi mereka? Bisakah kita melindungi mereka tanpa menghilangkan pilihan bagi orang-orang yang menggunakannya dengan bijaksana? Konsekuensi masa depan yang potensial negatif dari pilihan yang kita buat sekarang (seperti tidak mendapatkan olahraga yang cukup) adalah hal biasa dalam kehidupan. Kita dapat mendidik konsumen dan mendorong pilihan yang bertanggung jawab. (Pada akhir bab ini, kami mendaftar organisasi nirlaba yang membantu melakukan hal ini.) Penghormatan atas otonomi orang berarti membiarkan mereka membuat pilihan mereka sendiri. Merancang sistem secara etis dan bertanggung jawab berarti termasuk cara untuk menginformasikan dan mengingatkan pengguna tentang pengumpulan data yang tidak jelas, perubahan dalam kebijakan atau fitur, dan risiko.

**Membayar informasi konsumen**

Ketika bisnis pertama mulai membangun basis data konsumen yang luas, beberapa pendukung privasi berpendapat bahwa mereka harus membayar konsumen untuk menggunakan informasi mereka. Dalam banyak situasi, mereka (dan) membayar kami secara tidak langsung. Misalnya, ketika kami mengisi formulir pendaftaran kontes, kami memperdagangkan data untuk peluang memenangkan hadiah. Banyak bisnis memberikan diskon kepada pembeli yang menggunakan kartu yang memungkinkan pelacakan pembelian mereka. Banyak yang menawarkan untuk memperdagangkan produk dan layanan gratis untuk izin mengirim pesan iklan atau mengumpulkan informasi. Beberapa pendukung privasi mengkritik program-program semacam itu. LaurenWeinstein, pendiri Forum Privasi, berpendapat bahwa di antara orang yang kurang makmur, daya tarik layanan gratis mungkin sangat kuat, dan itu "memaksa" mereka untuk melepaskan privasi mereka.41 Orang tidak memahami semua potensi penggunaan informasi mereka dan konsekuensi jangka panjang dari perjanjian. Di sisi lain, program semacam itu menawarkan peluang bagi orang-orang dengan sedikit uang untuk memperdagangkan sesuatu yang bernilai (informasi) lainnya untuk barang dan jasa yang mereka inginkan. Free-PC memulai tren, pada tahun 1999, dengan tawaran 10.000 PC gratis dalam pertukaran untuk memberikan informasi pribadi dan menonton pesan iklan. Ratusan ribu orang membanjiri perusahaan dengan aplikasi di hari pertama.

Bagaimanapun, program awal ini dikerdilkan oleh perkembangan jejaring sosial, situs video gratis, dan sejumlah besar situs web lain yang memberikan informasi dan layanan secara gratis. Orang-orang mengerti bahwa iklan mendanai mereka. Gmail menargetkan iklan ke setiap pengguna dengan menganalisis pesan email pengguna. Beberapa pendukung privasi merasa ngeri: membaca email orang! Sebagai ganti izin untuk melakukannya, Gmail menyediakan email gratis dan layanan lainnya. Jutaan orang mendaftar. Keberhasilan bisnis dan layanan ini menunjukkan bahwa banyak orang tidak keberatan dengan pengecer menggunakan riwayat pembelian atau email mereka dan tidak menganggap intrusi iklan online sebagai hal yang sangat mengganggu, dan juga selancar Web mereka menjadi sangat sensitif. Apakah mereka memahami konsekuensi potensial?

### 2.3.2 Kegiatan Sosial dan Pribadi Kami

*Menyiarkan Diri Anda Sendiri.*

—Slogan di beranda YouTube

**Jejaring sosial — apa yang kita lakukan**

Ada dua aspek jaringan sosial yang perlu dipertimbangkan: tanggung jawab kita sendiri atas apa yang kita bagikan (bagaimana kita mengambil risiko privasi kita dan teman kita) dan tanggung jawab perusahaan yang menjadi tuan rumah kita informasi.

Banyak anak muda memposting pendapat, gosip, dan gambar yang dinikmati teman-teman mereka. Pos mereka dapat menimbulkan masalah jika orang tua, calon majikan, agen penegak hukum, atau berbagai orang lain melihatnya. Anak berusia 18 tahun yang memposting foto seksi dirinya dalam pakaian renang sedang memikirkan teman-temannya yang melihat mereka, bukan penguntit atau pemerkosa potensial. Orang yang mencoba membersihkan persona online mereka sebelum memulai pencarian kerja menemukan bahwa sulit untuk menghilangkan materi yang memalukan. Beberapa aplikasi jejaring sosial meminta informasi pribadi — seperti agama, pandangan politik, dan orientasi seksual — tentang teman seseorang dan juga diri sendiri. Apakah orang-orang berpikir tentang bagaimana informasi itu dapat digunakan dan apakah teman-teman mereka ingin mengungkapkannya?

Mengapa begitu lama praktik standar untuk menghentikan pengiriman surat dan surat kabar ketika pergi bepergian? Satu detail tentang lokasi ini ("jauh dari rumah") adalah penting untuk melindungi dari pencuri yang potensial. Namun, sekarang, banyak sekali orang yang memposting lokasi mereka (dan teman-teman mereka) ke jejaring sosial.

Jaringan sosial, dengan ratusan atau ribuan teman jaringan yang tidak pernah mereka temui, mungkin tidak cukup memikirkan implikasi dari informasi pribadi yang mereka sediakan. Ketika seseorang pada awalnya memilih pengaturan privasi, akankah orang itu kemudian ingat siapa yang mendapatkan laporan waktu nyata tentang status dan aktivitasnya?

Instansi pemerintah dan bisnis melakukan banyak hal yang salah, tetapi individu juga tidak selalu melakukan pemikiran dan perawatan yang tepat untuk privasi, masa depan, dan keselamatan mereka sendiri.

*Jajak pendapat menunjukkan bahwa orang-orang peduli dengan privasi.*

*Mengapa mereka tidak bertindak seperti itu?*

—Ian Kerr

**Jejaring sosial — apa yang dapat mereka lakukan**

Kami menggunakan Facebook untuk contoh kami di sini karena memiliki begitu banyak fitur dan begitu banyak

anggota, dan karena itu telah membuat kesalahan instruktif. Prinsip-prinsip ini berlaku untuk media sosial lain dan situs web lain.

Facebook secara teratur memperkenalkan layanan baru, cara-cara baru untuk berbagi dengan teman-teman dan tetap up-to-date pada aktivitas mereka. Beberapa kali, Facebook secara serius salah menilai bagaimana anggota akan bereaksi dan membuat pilihan yang buruk. Beberapa contoh yang kami gambarkan dengan cepat menimbulkan kritik dari puluhan ribu hingga ratusan ribu anggota serta dari pendukung privasi.

Umpan berita mengirim perubahan terbaru dalam informasi pribadi anggota, daftar teman, dan kegiatan kepada teman-teman anggota tersebut.44 Facebook mengatakan tidak mengubah pengaturan privasi ketika memperkenalkan feed. Ini mengirimkan informasi hanya kepada orang-orang yang sudah disetujui oleh anggota dan siapa yang sudah bisa melihatnya jika mereka melihat. Dalam satu atau dua hari, ratusan ribu anggota Facebook memprotes dengan penuh semangat. Mengapa? Kemudahan mengakses informasi kadang-kadang bisa lebih penting daripada fakta bahwa itu tersedia di suatu tempat. Banyak orang tidak memeriksa ratusan teman mereka secara teratur. Namun, feed tersebut menyebarkan informasi ke semua orang secara instan. Berikut ini hanya satu jenis contoh yang membuat perbedaan: Di dunia fisik, kami mungkin membagikan informasi tentang akhir hubungan, penyakit serius, atau masalah keluarga dengan beberapa , dipilih, teman dekat. Secara bertahap, ketika kita menyesuaikan diri dengan situasi baru, yang lain mungkin belajar dari peristiwa tersebut. Umpan menghapus penundaan yang bersifat emosional.

Ketika Facebook mulai memberi tahu anggota tentang pembelian teman-teman mereka, masalah berkisar dari memanjakan hadiah kejutan hingga pengungkapan yang memalukan dan mengkhawatirkan. Haruskah Facebook memperkenalkan fitur-fitur seperti itu berubah menjadi “on” untuk semua orang? Atau haruskah perusahaan mengumumkannya dan membiarkan anggota memilih dengan klik? Ketika Facebook memperkenalkan alat pengenalan wajah untuk membantu anggota menandai teman di foto, defaultnya adalah alat itu aktif untuk semua anggota. Ada cara untuk tidak ikut serta, tetapi banyak pengguna yang tidak mengetahui fitur baru tersebut, jadi mereka tidak tahu untuk tidak memilih. Fitur Facebook's Place memungkinkan pengguna menandai teman-teman yang ada di lokasinya (apakah teman itu benar-benar ada). Apa yang seharusnya menjadi pengaturan default?

Anggota yang marah tidak baik untuk bisnis. Insiden-insiden ini menunjukkan pentingnya, baik dari perspektif etika dan perspektif bisnis, memberikan pemikiran yang cermat terhadap implikasi dan risiko fitur baru dan pemilihan pengaturan default. Perubahan yang mungkin tampak kecil dan halus dapat berdampak besar pada persepsi pribadi tentang privasi, risiko, dan perasaan nyaman. Orang-orang mungkin akan senang jika beberapa teman menandai mereka dalam beberapa foto, tetapi mereka mungkin sangat tidak nyaman jika sistem otomatis menandai setiap foto yang ditampilkan. Kuantitas dapat membuat perbedaan dalam kualitas yang dirasakan (khususnya, dalam perasaan kontrol seseorang informasi tentang diri sendiri). Dalam lingkungan yang kompleks, seperti jaringan sosial dengan banyak fitur dan anggotanya, kebijakan keikutsertaan lebih disukai — yaitu, kebijakan di mana anggota harus secara eksplisit mengaktifkan fitur tersebut, atau jika tidak tetap aktif. Dalam lingkungan yang kompleks, itu juga berharga untuk memiliki berbagai opsi. Misalnya, untuk fitur pemberian tag (untuk lokasi atau foto), opsi dapat mencakup memberi tahu orang tersebut dan memungkinkan penghapusan tag, meminta izin untuk setiap tag sebelum ditayangkan, dan memungkinkan anggota untuk sepenuhnya keluar dari tag. (Facebook memodifikasi Places untuk memasukkan berbagai tingkat perlindungan.)

Menurut Federal Trade Commission (FTC), Facebook melanggar kebijakan yang dinyatakan dalam beberapa contoh: dengan memberikan ID pengguna kepada pengiklan bersama dengan data pada aktivitas pengguna, dengan mengizinkan ketiga -party aplikasi akses penuh ke data pribadi anggota, dan dengan tidak menghapus beberapa data anggota ketika anggota menghapus akun. Tindakan seperti itu, yang melanggar pernyataan perusahaan sendiri tentang praktiknya, bersifat menipu; mereka menggagalkan keputusan dan kesepakatan yang diinformasikan. Kita mungkin tidak menyukai, mencela, berdebat, dan tidak setuju tentang etika beberapa praktik data. Praktik yang menipu lebih jelas tidak etis (atau tidak etis pada tingkat yang lebih kuat) daripada salah atau secara sembarangan membuat pilihan yang buruk tentang default.

**Tanggung jawab dari layanan gratis**

Kita harus menghargai jumlah layanan gratis yang luar biasa yang tersedia bagi kita dari perusahaan jejaring sosial — serta mesin pencari, sistem komunikasi seperti Twitter, situs web yang penuh dengan informasi ahli, dan sebagainya. Kita bisa memilih untuk menggunakannya atau tidak. Pada saat yang sama, bisnis yang menjalankan layanan gratis ini memiliki tanggung jawab kepada penggunanya. Jika Anda mengundang tetangga Anda untuk menggunakan mobil Anda kapan saja mereka inginkan tanpa bertanya, Anda memiliki tanggung jawab etis untuk tidak meninggalkan kunci di mobil saat rem tidak berfungsi. Tidak masalah jika Anda tidak memungut biaya. Perusahaan mungkin tidak, secara etis, menawarkan layanan yang menarik dan kemudian menyebabkan risiko bahaya yang signifikan, terutama ketika risiko disembunyikan atau tidak terduga.

**Kehidupan di dunia maya**

Segera setelah seorang wanita mulai menulis blog pribadi, dia menemukan bahwa seseorang yang tidak dia temui selama bertahun-tahun membacanya. Ini membuatnya ngeri. Mungkin dia berpikir hanya orang yang dia beri alamat Web yang membaca blog. Dia tidak menyadari bahwa itu muncul tinggi dalam hasil pencarian untuk namanya.45 Wanita lain menyukai fitur di situs jejaring sosial yang memberi tahu anggota yang mana yang membaca profilnya. Dia terkejut dan kesal karena menemukan bahwa orang-orang yang profilnya dia baca tahu bahwa dia membacanya. Setelah Facebook menyarankan bahwa dua wanita mungkin ingin berteman, salah satu dari mereka menemukan bahwa mereka berdua menikah dengan pria yang sama.

Insiden pertama mengingatkan kita bahwa beberapa orang tidak tahu atau cukup mengerti tentang bagaimana theWeb bekerja untuk membuat keputusan yang baik tentang apa yang harus diletakkan di sana.*\_* Yang kedua menunjukkan bahwa beberapa orang tidak memikirkannya dengan hati-hati. Ini juga menggambarkan fenomena yang sangat umum: orang sering menginginkan banyak informasi tentang orang lain, tetapi mereka tidak ingin orang lain memiliki akses ke jenis informasi yang sama tentang diri mereka. The bigamist tidak menyadari bahwa Facebook akan melihat kedua istrinya memiliki kesamaan.

Beberapa orang memasukkan tanggal lahir mereka di profil online atau di r´esum´es yang mereka posting di situs pencari kerja. Situs genealogi sangat populer. Orang-orang membuat pohon keluarga dengan profil lengkap anggota keluarga, termasuk tanggal lahir dan nama gadis ibu. Institusi medis dan keuangan menggunakan informasi yang sama ini (tanggal lahir dan nama gadis ibu) untuk memverifikasi identitas pelanggan. Kami dapat mengubah kata sandi yang diungkapkan; kita tidak bisa mengubah tanggal lahir atau nama gadis ibu kita.

Web bersifat publik. Kebanyakan orang layak dan tidak berbahaya, tetapi banyak yang jahat dan berbahaya. Pedofil memiliki situs web yang tertaut ke situs-situs Pramuka, Brownies (versi muda Pramuka), tim sepak bola SMP, dan seterusnya — situs dengan foto anak-anak dan kadang-kadang nama dan informasi pribadi lainnya. Itu menakutkan. Itu tidak berarti bahwa organisasi semacam itu tidak boleh menempatkan gambar di situs web mereka. Ini menunjukkan, bagaimanapun, bahwa mereka mempertimbangkan apakah akan memasukkan nama-nama anak-anak, apakah perlu pendaftaran untuk penggunaan situs, dan sebagainya.

Bertahun-tahun yang lalu, ketika banyak rumah memiliki mesin penjawab yang terhubung ke telepon, beberapa orang, sebaliknya, menggunakan layanan penjawab. Pesan yang tersisa untuk mereka tinggal di mesin rekaman di situs bisnis layanan. Saya ingat betapa terkejutnya saya bahwa orang-orang merasa nyaman memiliki pesan pribadi mereka pada mesin di luar kendali mereka. Betapa kuno dan tua-

*\_* Dalam contoh inisiatif yang tidak biasa, wanita itu mempelajari teknik yang digunakan untuk menentukan peringkat hasil pencarian dan memodifikasi

blognya sehingga tidak lagi muncul secara mencolok dalam pencarian namanya.

dibentuk kekhawatiran yang tampaknya sekarang. Ponsel dan pesan email kami secara rutin berada di komputer di luar rumah atau kantor kami. Pesan teks dapat diambil beberapa bulan kemudian. Setelah banyak insiden pemaparan pesan yang memalukan, kita masih melihat individu, politisi, pengacara, selebritis, dan pebisnis menulis hal-hal yang sensitif, kasar, atau berkompromi dalam email, teks, dan tweet dengan keyakinan yang jelas bahwa tidak seorang pun kecuali penerima yang dituju akan pernah Lihat mereka.

Jutaan orang Amerika mempersiapkan pengembalian pajak mereka secara online. Apakah mereka berpikir tentang ke mana data pendapatan dan pengeluaran mereka pergi? Berapa lama data tetap online? Seberapa baik mengamankan datanya? Usaha kecil menyimpan semua informasi akuntansi online mereka (di "cloud") di situs yang menyediakan layanan dan akses akuntansi dari mana saja. Apakah pemilik bisnis memeriksa keamanan situs-situs tersebut? Beberapa situs web medis menyediakan tempat yang mudah bagi orang untuk menyimpan catatan medis mereka. Berbagai perusahaan menawarkan layanan di mana orang menyimpan semua data mereka (email, foto, kalender, file) di server perusahaan, bukan di PC atau laptop mereka sendiri. Anda dapat menyimpan inventaris properti berharga Anda di Web (gratis) untuk membantu klaim asuransi setelah kebakaran atau angin puting beliung. Perusahaan yang memasok layanan ini mungkin jujur, tetapi data, jika bocor atau diretas, adalahbelanja

daftarbagi pencuri.

Ada keuntungan besar untuk semua layanan ini. Mereka nyaman. Kami tidak harus mengelola sistem kami sendiri. Kami tidak perlu melakukan backup. Kita bisa mendapatkan file-file kita dari mana saja dengan akses Internet. Kita dapat lebih mudah berbagi file dan berkolaborasi dengan orang lain dalam proyek. Ada kerugian juga. Kami tidak dapat mengakses file kami ketika jaringan mati atau jika ada masalah teknis di perusahaan yang menyimpannya. Tetapi risiko yang lebih serius adalah privasi dan keamanan. Kami kehilangan kendali. Di luar rumah kami, file kami berisiko kehilangan, pencurian, penyalahgunaan oleh karyawan, pemaparan yang tidak disengaja, penyitaan oleh lembaga pemerintah, penggunaan oleh penyedia layanan yang dijelaskan dalam perjanjian atau kebijakan privasi yang tidak kami baca, menggunakan kami diabaikan ketika mendaftar untuk layanan, dan kemudian menggunakan yang tidak ada yang diantisipasi. Kami mungkin tidak peduli siapa lagi yang melihat foto liburan kami. Kami mungkin memutuskan kenyamanan mengisi formulir pajak secara online atau menyimpan catatan medis kami secara online melebihi risikonya. Intinya adalah sadar dan membuat keputusan secara sadar. Untuk profesional komputer, kesadaran akan risiko harus mendorong perawatan dan tanggung jawab dalam mengembangkan sistem yang aman untuk melindungi informasi sensitif yang disimpan orang secara online.

### 2.3.3 Pelacakan Lokasi

Sistem penentuan posisi global (GPS), ponsel, identifikasi frekuensi radio (RFID) tag,*\_* dan teknologi dan perangkat lain memungkinkan berbagai aplikasi berbasis lokasi — yaitu, layanan komputer dan komunikasi yang bergantung pada mengetahui di mana tepatnya seseorang atau benda pada waktu tertentu. Sejak diperkenalkannya iPhone, telah terjadi ledakan pada aplikasi semacam itu. Aplikasi yang luar biasa beragam

*\_* tag RFID adalah perangkat kecil yang berisi chip elektronik dan antena. Chip menyimpan data identifikasi

(dan mungkin data lain) dan mengontrol pengoperasian tag. Antena mentransmisikan dan menerima sinyal radio untuk

berkomunikasi dengan perangkat yang membaca tag.

dan memiliki manfaat yang signifikan. Namun, mereka menambahkan informasi terperinci tentang lokasi kami saat ini dan pergerakan kami di masa lalu ke kumpulan informasi yang disimpan oleh sistem komputer tentang kami, dengan semua potensi ancaman terhadap privasi.

Untuk menganalisis risiko, kita harus selalu mempertimbangkan penggunaan yang tidak diinginkan, sebagaimana yang dimaksudkan. Ingat dari Bagian 2.2.2 bahwa lembaga penegak hukum menemukan orang dengan menempatkan telepon mereka. Rincian teknologi bersifat rahasia dan perangkatnya mungkin mahal. Tapi itu hanya sementara. Akhirnya akan ada aplikasi untuk itu. Jadi bayangkan bahwa siapa pun dapat memasukkan nomor ID seseorang (mungkin nomor telepon) di perangkat seluler mereka dan tanyakan di mana orang itu sekarang. Atau mungkin perangkat dapat menyapu lokasi tertentu dan mendeteksi perangkat identifikasi orang-orang di sana — atau mengidentifikasi mereka dengan pengenalan wajah. Siapa yang mungkin *tidak* ingin mendapatkan informasi ini? Pencuri. Pasangan kekerasan atau mantan pasangan. Seorang pengacara perceraian. Tetangga yang menjengkelkan atau usil. Penguntit. Rekan kerja atau rekan bisnis. Siapa pun yang mungkin keberatan dengan agama, politik, atau perilaku seksual Anda. Pemerintah. (Oh, kami melihat bahwa guru baru kami berada di pertemuan Alcoholics Anonymous. Siapa yang ada di toko mariyuana medis atau toko senjata sekarang?) Catatan ekstensif tentang di mana kami memberikan rincian lebih lanjut untuk profil dan bisnis arsip yang terus berkembang dan pemerintah membangun tentang kita. Dengan alat penelusuran, pencocokan, dan analisis yang cepat, mereka dapat menambahkan lebih banyak detail tentang siapa yang menghabiskan waktu bersama dan apa yang kita lakukan. Dalam Bab 1, kami menyebutkan bahwa para peneliti belajar tentang organisasi sosial dan penyebaran penyakit (antara lain) dengan mempelajari sejumlah besar data ponsel. Data statistik seperti itu dapat sangat berharga bagi kita semua, tetapi ponsel mengidentifikasi seseorang, dan, dengan demikian, informasi pelacakan (jika dikaitkan dengan nomor telepon atau ID) adalah informasi pribadi dan memunculkan masalah persetujuan yang biasa, penggunaan sekunder potensial, risiko penyalahgunaan, dan sebagainya. Perawatan harus diambil untuk memastikan bahwa data tersebut dilindungi. Jika diakses secara diam-diam, dicuri, diungkapkan secara tidak sengaja, atau diperoleh oleh instansi pemerintah, catatan lokasi dan gerakan kami menimbulkan ancaman terhadap privasi, keselamatan, dan kebebasan. Privasi dan organisasi industri mengembangkan panduan untuk penggunaan aplikasi pelacakan lokasi untuk menerapkan prinsip-prinsip pada Gambar 2.2 dan melindungi terhadap beberapa risiko.

Mempelajari perilaku pelanggan di toko atau fasilitas lain adalah aplikasi potensi besar dari pelacakan lokasi. Misalnya, supermarket atau taman hiburan mungkin ingin menganalisis pola lalu lintas pelanggan di dalam fasilitas untuk merencanakan tata letak yang lebih baik, untuk menentukan berapa banyak waktu yang dihabiskan orang di dalam, atau untuk menganalisis waktu tunggu. Implikasi privasi dan risiko pemantauan gerakan orang bervariasi dari sedikit ke besar tergantung pada bagaimana sistem pelacakan melakukan tugasnya. Anggaplah, misalnya, taman hiburan seperti Disneyland ingin mempelajari pola lalu lintas pengunjung, mendeteksi keramaian dan garis panjang, dan sebagainya. Hal ini dapat dilakukan dengan tiket pemancar lokasi yang didapatkan orang ketika mereka masuk dan membuang ketika mereka pergi. Tidak perlu ada informasi yang terhubung dengan orang atau keluarga. Untuk sistem seperti itu, privasi bukanlah masalah. Akan ada godaan, bagaimanapun, untuk memasukkan data demografi dan mungkin mengidentifikasi data pada pelacak.

**Siapa yang ada di dalam Bar?**

Ratusan bar memasang kamera dengan sistem pengenalan wajah untuk menyediakan data ke situs web dan aplikasi ponsel cerdas. Aplikasi ini memberi tahu pengguna jumlah orang di bar tertentu, rasio pria / wanita, dan rentang usia perkiraan. Setiap batang mendapat ringkasan statistik tentang pelanggannya yang dapat berguna untuk iklan atau perencanaan bisnis lainnya. Sistem tidak mengidentifikasi individu dan tidak menyimpan video. Jadi ini bukan masalah privasi. Atau itu? Intinya adalah bahwa aplikasi semacam itu dapat tetap sama sekali tidak mengancam, atau dapat melayang melewati batas ke dalam pelacakan lokasi dan pelanggaran privasi. Pemilik bar tidak mengontrol sistem, sehingga mereka tidak dapat memastikan bahwa apa yang mereka katakan kepada pelanggan mereka tentang itu adalah benar. (Ada banyak contoh sistem yang mengumpulkan dan menyimpan data tanpa sepengetahuan bisnis yang menggunakan sistem.) Pengembang dan operator sistem mungkin sangat berhati-hati untuk melindungi privasi pelanggan, atau mereka mungkin menyerah pada godaan untuk menambahkan fitur baru yang membutuhkan penyimpanan video atau mengidentifikasi individu. Kesadaran akan potensi risiko dan pemahaman praktik privasi yang baik sangat penting bagi pengembang perangkat lunak yang menciptakan dan meningkatkan sistem tersebut dan manajer yang membuat keputusan tentang fitur apa yang harus diterapkan.

**Alat untuk para orang tua**

Banyak teknologi membantu orang tua melacak lokasi fisik anak-anak mereka. Layanan telepon seluler memungkinkan orang tua memeriksa lokasi anak dari perangkat seluler orang tua. Layanan yang dipasang di mobil memberi tahu orang tua tempat remaja mereka berada dan seberapa cepat mereka mengemudi. Sebuah perusahaan menjual pemancar gelang nirkabel untuk anak-anak, sehingga orang tua dapat memantaunya. Tag RFID di sepatu dan pakaian bisa dipantau ratusan meter jauhnya. Ini mungkin sangat membantu dengan anak-anak muda yang berkeliaran di tempat yang ramai.

Melacak anak-anak dapat meningkatkan keamanan, tetapi ada masalah pengasuhan dan risiko yang terlibat dalam menggunakan alat pelacak. Pada usia berapa pelacakan menjadi pelanggaran privasi anak? Haruskah orang tua memberi tahu anak-anak tentang perangkat dan layanan pelacakan yang mereka gunakan? Informed consent adalah prinsip dasar untuk orang dewasa. Pada usia berapa itu berlaku untuk anak-anak? Apakah pelacakan dan pemantauan yang intensif memperlambat perkembangan kemandirian seorang anak yang bertanggung jawab?

Sistem pemantauan yang mengirim sinyal yang mudah dibaca atau mudah disadap dapat menurunkan alih-alih meningkatkan keselamatan seorang anak. Penganiaya anak dan pencuri identitas bisa mengumpulkan data pribadi. Orangtua perlu menyadari potensi alarm palsu dan rasa aman yang salah. Misalnya, seorang anak mungkin kehilangan ponsel atau meninggalkan artikel yang ditandai di suatu tempat. Anak-anak yang lebih tua mungkin mencari cara untuk menggagalkan sistem pelacakan. Jelas, bagaimana dan kapan menggunakan alat pengawasan harus melibatkan keputusan yang bijaksana untuk keluarga.

Hewan peliharaan, tahanan, dan orang-orang dengan penyakit Alzheimer dapat memakai perangkat yang menemukan mereka jika mereka berkeliaran. Veterinarians menanamkan chip ID di bawah kulit hewan peliharaan dan hewan ternak.

**Menggagalkan pemburu, mengikuti kura-kura, melacak gitar**

Pemilik menandai tanaman yang sangat berharga dan sangat langka, baik di alam liar maupun di kebun, dengan melacak chip sehingga mereka dapat menemukannya jika dicuri. Teknologi satelit dan mikroprosesor sangat meningkatkan pelacakan hewan. Para ilmuwan sekarang memasang pemancar kecil untuk burung langka dan hewan lain untuk mempelajari perilaku mereka dan belajar bagaimana melindungi sumber makanan mereka. Para peneliti mengetahui bahwa beberapa hewan melakukan perjalanan jauh lebih jauh dari yang diperkirakan sebelumnya: Penyu laut berenang dari Karibia ke Afrika. Elang laut yang bersarang terbang dari Hawaii ke Teluk San Francisco, perjalanan pulang pergi sepanjang minggu, untuk mendapatkan makanan bagi anak-anaknya. Untuk mendorong minat dari masyarakat, para peneliti membuat situs web di mana kita dapat mengikuti gerakan binatang. Ini adalah layanan berharga. Apa yang terjadi ketika teknologi yang sama melacak orang? Saya baru-baru ini melakukan tur pabrik gitar. Pemandu tur menunjukkan kepada kita leher gitar yang sebagian lengkap. Dan di sana, di bagian depan leher, ada chip RFID. Papan fret, ketika

terpasang ke leher, menutupi chip. Panduan itu menjelaskan betapa berguna chip itu untuk melacak gitar melalui produksi dan untuk menemukan gitar khusus di ruang stok. Chip tetap di gitar ketika pelanggan membelinya. Produsen menempatkan tag RFID di banyak produk lain, selain gitar, untuk melacaknya melalui proses manufaktur dan penjualan. Apa potensi untuk melacak orang melalui produk yang mereka beli? Apakah itu penting? Beberapa orang menyarankan untuk melakukan ini untuk tahanan dan anak-anak. Apakah saran untuk memasang chip pelacakan pada orang membuat Anda bertanya-tanya apakah itu ide yang bagus? Setelah oposisi berat dari orang tua, sebuah sekolah membatalkan proposal untuk mengharuskan semua siswa memakai perangkat yang dilengkapi dengan RFID saat berada di sekolah. Pengawasan konstan dan risiko penyalahgunaan cukup, dalam pikiran banyak orang tua, untuk melebihi manfaat dari alat pelacak yang dapat dilepas.

**2.3.4 Hak untuk Dilupakan**

Orang terkadang ingin menghapus informasi tentang diri mereka dari Internet atau dari catatan perusahaan. Ini bisa menjadi komentar ofensif yang dibuat dalam kemarahan, foto di halaman jejaring sosial sendiri atau situs berbagi foto, informasi dalam direktori online, atau data pribadi yang diposting oleh orang lain (misalnya, di situs silsilah). Bisa jadi profil perusahaan periklanan yang dikembangkan dengan melacak aktivitas Web seseorang, kumpulan data yang dikumpulkan dari penggunaan ponsel cerdas seseorang, atau kumpulan kueri penelusuran orang yang disimpan toko mesin. Ini bisa menjadi gambar atau informasi yang tidak menarik yanglain diposting orang. Mungkin tautan mesin telusur ke materi semacam itu. Legislator danprivasi pendukungdi Amerika Serikat dan Uni Eropa mempromosikan hak hukum untuk menuntut agar situs web menghapus materi tentang diri sendiri.

Hak untuk menghapus materi, sebagai hak legal atau etis, telah disebut “hak untuk dilupakan.” Materi yang luas yang mungkin ingin dihapus oleh seseorang menunjukkan banyak pertanyaan praktis, etis, sosial, dan hukum dan kritik tentang hak seperti itu.

Kebijakan berbagai situs web tentang penghapusan materi bervariasi. Beberapa situs dengan anggota, seperti jejaring sosial, menanggapi permintaan anggota untuk menghapus materi yang diposkan pengguna dan menghapus materi anggota saat anggota menutup akun. Ketika materi tidak ada dalam akun pengguna, situasinya menjadi lebih rumit. Beberapa situs, seperti direktori, mengumpulkan informasi secara otomatis; dengan demikian, informasi yang dihapus dapat muncul kembali. Sistem filter untuk mencegah pengeposan ulang untuk orang tertentu memiliki masalah membedakan dengan tepat orang itu dari orang lain dengan nama yang sama atau mirip.

Haruskah perusahaan atau situs web selalu mematuhi permintaan untuk menghapus item tertentu atau catatan seseorang kapan pun seseorang membuat permintaan semacam itu? Kami memahami bahwa orang-orang melakukan hal-hal bodoh dan menyesalinya kemudian. Masuk akal membiarkan banyak dari mereka dilupakan. Jika seseorang ingin menghapus sesuatu yang dia posting di situs web, itu masuk akal, sopan, bersemangat, dan mungkin kebijakan bisnis yang baik untuk dipatuhi. Jika orang lain memposting foto atau informasi yang dikompromikan dari masa lalu seseorang, menghapusnya menimbulkan masalah kebebasan berbicara dan kebenaran. Jika orang tersebut bukan figur publik dan informasi tersebut tidak memiliki nilai sosial yang luas, menghapusnya mungkin hal yang wajar dan sopan untuk dilakukan. Mematuhi permintaan dapat diterima secara etis dan mengagumkan tetapi tidak secara etika wajib. Dalam beberapa kasus, itu bisa menjadi ide yang buruk. Informasi itu mungkin penting bagi orang-orang dalam komunitas tertentu. Orang yang mempostingnya mungkin memiliki alasan yang bagus. Keputusan yang tepat dalam kasus tertentu mungkin sulit.

Bagaimana dengan data yang dikumpulkan pengiklan dan mesin pencari tentang kami? Haruskah mereka, dari sudut pandang etika, mematuhi permintaan dari seseorang yang ingin catatannya dihapus? Jika perusahaan mengumpulkan data secara diam-diam, tanpa izin, atau melanggar kebijakan privasi dan ketentuan penggunaan yang mereka nyatakan, maka ada alasan bagus untuk meminta penghapusannya terlepas dari hak apa pun untuk dilupakan. Anggaplah informasi tersebut adalah kumpulan kueri penelusuran seseorang atau sesuatu yang serupa yang dikumpulkan oleh situs web gratis, dan anggap situs tersebut mengumpulkan dan menggunakan data yang jelas dalam ketentuan penggunaannya. Penggunaan data oleh perusahaan adalah, sebagian, pembayaran kami untuk layanan gratis yang disediakannya. Jika perusahaan setuju untuk menghapus catatan orang atas permintaan, itu memberikan layanannya kepada orang-orang itu secara gratis (atau dengan "diskon" jika mereka terus melihat iklan di situs). Jika sejumlah kecil individu meminta penghapusan data mereka, perusahaan besar mungkin dapat mematuhi tanpa ketidaknyamanan yang signifikan atau pengurangan nilai yang didapat dari analisis data pengguna. Banyak perusahaan memberikan beberapa produk dan layanan secara gratis. Sekali lagi, memenuhi permintaan penghapusan dapat secara etis dan sosial mengagumkan, bersemangat, dan mungkin kebijakan bisnis yang baik. Di sisi lain, seseorang mungkin membuat permintaan penghapusan untuk menyembunyikan beberapa perilaku ilegal atau ofensif atau untuk menghapus bukti dalam sengketa sejenis.

Jika hak untuk dilupakan adalah hak negatif (kebebasan), itu bisa berarti bahwa kita dapat memilih untuk menjauhi Internet dan menjadi pertapa, tetapi kita tidak bisa memaksa orang lain untuk menghapus foto yang kita masuki. Sebagai positif benar (hak klaim), itu sama dengan mengharuskan orang lain menghapus pikiran mereka, serta foto, blog, dan tautan mereka. Itu bisa berarti bahwa orang lain tidak boleh menulis tentang seseorang atau menukarkan informasi tertentu tentang orang itu — informasi yang diperoleh tanpa melanggar hak-hak orang tersebut. Ini dapat melanggar kebebasan berbicara. Dalam beberapa aplikasi, hak akan berarti bahwa seseorang dapat melanggar perjanjian (misalnya, syarat penggunaan untuk layanan Web) sesuka hati. Tampaknya ada sedikit jika ada dasar untuk hak etis seperti itu.

Apakah ada konteks di mana masuk akal untuk menegakkan persyaratan hukum untuk menghapus materi ketika seseorang memintanya? Mungkin untuk populasi khusus, seperti anak-anak (di mana orang tua mungkin membuat permintaan atau orang dewasa muda mungkin ingin menghapus foto sexting seminude yang dikirim ke teman saat di sekolah menengah). Mungkin dalam situasi khusus lainnya. Legislator harus dengan hati-hati menyusun persyaratan hukum seperti itu untuk menghindari konflik dengan kebebasan berbicara, aliran informasi gratis, dan perjanjian kontraktual. Persyaratan hukum untuk memenuhi permintaan penghapusan akan lebih membebani situs kecil daripada yang besar, yang dapat mengembangkan perangkat lunak untuk membantu mengotomatiskan proses dan memiliki staf hukum untuk mempertahankan diri dari keluhan.

## 2.4 Sistem Pemerintahan

### 2.4.1 Basis Data

Instansi pemerintah federal dan lokal memelihara ribuan basis data yang berisi informasi pribadi. Contohnya termasuk pajak, kepemilikan properti, medis, perjalanan, perceraian, pendaftaran pemilih, kebangkrutan, dan catatan penangkapan. Yang lainnya termasuk aplikasi untuk program hibah pemerintah dan pinjaman, lisensi profesional dan perdagangan, dan catatan sekolah (termasuk tes psikologis anak-anak). Dan masih banyak lagi. Database pemerintah membantu lembaga pemerintah menjalankan fungsinya, menentukan kelayakan untuk program tunjangan pemerintah, mendeteksi penipuan dalam program pemerintah, mengumpulkan pajak, dan menangkap orang yang melanggar hukum. Ruang lingkup kegiatan pemerintah sangat besar, mulai dari menangkap penjahat yang kejam hingga melisensikan penata bunga. Pemerintah dapat menangkap orang, memenjarakan mereka, dan menyita aset dari mereka. Dengan demikian, penggunaan dan penyalahgunaan data pribadi oleh lembaga pemerintah menimbulkan ancaman khusus terhadap kebebasan dan privasi pribadi. Tampaknya masuk akal untuk mengharapkan pemerintah untuk memenuhi standar sangat tinggi untuk perlindungan privasi dan kepatuhan terhadap aturan mereka.

Privacy Act of 1974 adalah hukum utama tentang penggunaan data pribadi oleh pemerintah federal. Ringkasan ketentuan Undang-Undang muncul pada Gambar 2.3. Meskipun undang-undang ini merupakan langkah penting dalam upaya melindungi privasi kita dari penyalahgunaan oleh agen federal, ini memiliki masalah. Undang-Undang Privasi memiliki, mengutip satu pakar tentang undang-undang privasi, “banyak celah, penegakan yang lemah, dan hanya pengawasan sporadis.”49 E-GovernmentAct 2002 menambahkan beberapa peraturan privasi untuk data dan layanan elektronik — misalnya, yang mewajibkan lembaga

* Membatasi data dalam catatan pemerintah federal untuk apa yang "relevan dan perlu" untuk tujuan hukum yang pemerintah mengumpulkannya
* . Membutuhkan agen federal untuk mempublikasikan pemberitahuan sistem catatan mereka dalam Daftar Federal sehingga publik dapat belajar tentang database apa yang ada
* . Memungkinkan orang untuk mengakses catatan mereka dan memperbaiki informasi yang tidak akurat
* . Memerlukan prosedur untuk melindungi keamanan informasi dalam basis data
* . Melarang pengungkapan informasi tentang seseorang tanpa persetujuannya (dengan beberapa pengecualian)

**Gambar 2.3** Ketentuan dari Undang-undang Privasi 1974.

untuk melakukan penilaian dampak privasi untuk sistem informasi elektronik dan untuk memposting kebijakan privasi di situs web agensi yang digunakan oleh publik.

Government Accountability Office (GAO) adalah "lembaga pengawas" Kongres. Selama 25 tahun terakhir, GAO telah mengeluarkan banyak penelitian yang menunjukkan kurangnya kepatuhan terhadap Undang-undang Privasi dan risiko serta pelanggaran privasi lainnya. GAO melaporkan pada tahun 1996 bahwa staf Gedung Putih menggunakan database "rahasia" dengan catatan pada 200.000 orang (termasuk informasi etnis dan politik) tanpa kontrol akses yang memadai. Sebuah studi GAO dari 65 situs web pemerintah menemukan bahwa hanya 3% dari situs yang sepenuhnya memenuhi standar informasi yang adil untuk pemberitahuan, pilihan, akses, dan keamanan yang ditetapkan oleh Federal Trade Commission (FTC) untuk situs web komersial. (Situs FTC adalah salah satu yang tidak sesuai.) GAO melaporkan bahwa Internal Revenue Service (IRS), Biro Investigasi Federal (FBI), Departemen Luar Negeri, dan lembaga lain yang menggunakan data mining untuk mendeteksi penipuan atau terorisme melakukan tidak mematuhi semua aturan untuk mengumpulkan informasi tentang warga negara. GAO menemukan lusinan kelemahan dalam pengoperasian jaringan komunikasi pemerintah untuk mentransmisikan data medis dalam program Medicare dan Medicaid - kelemahan yang dapat memungkinkan akses tanpa izin ke catatan medis masyarakat.

IRS adalah salah satu dari beberapa lembaga pemerintah federal yang mengumpulkan dan menyimpan informasi tentang hampir semua orang di negara ini. Ini juga merupakan pengguna sekunder utama dari informasi pribadi. Tahun demi tahun, ratusan karyawan IRS diselidiki karena pengintaian yang tidak sah dalam file pajak orang. (Seorang karyawan IRS yang merupakan anggota Ku Klux Klan membaca catatan pajak anggota kelompok Klan-nya mencari informasi pendapatan yang akan menunjukkan bahwa seseorang adalah agen yang menyamar.) Pelanggaran ini menyebabkan hukum dengan hukuman berat bagi pegawai pemerintah yang mengintip melalui informasi pajak orang tanpa otorisasi. Namun, laporan GAO beberapa tahun kemudian menemukan bahwa sementara IRS telah melakukan perbaikan signifikan, badan pajak masih gagal melindungi informasi keuangan dan pajak orang. Karyawan IRS dapat mengubah dan menghapus data tanpa otorisasi. Karyawan membuang disk dengan informasi pembayar pajak yang sensitif tanpa menghapus file. Ratusan kaset dan disket hilang. Sebuah laporan oleh Inspektur Jenderal Departemen Keuangan mengatakan bahwa IRS tidak cukup melindungi informasi pembayar pajak di lebih dari 50.000 laptop dan media penyimpanan lainnya. Informasi keuangan pribadi yang diberikan oleh pembayar pajak kepada IRS adalah "berisiko" dari para peretas dan karyawan yang tidak puas karena banyak dari 250 lembaga negara bagian dan federal di mana IRS memberikan informasi pembayar pajak tidak memiliki perlindungan yang memadai.51

Berbagai tinjauan kepatuhan terhadap Undang-Undang Privasi dan Undang-Undang E-Government telah menyoroti kelemahan dalam undang-undang ini. GAO menganjurkan untuk memodifikasi Undang-Undang Privasi untuk mencakup semua informasi identitas pribadi yang dikumpulkan dan digunakan oleh pemerintah federal, sehingga menutup celah yang menganga yang mengecualikan banyak penggunaan informasi pribadi oleh pemerintah dari ketentuan hukum. GAO mengadvokasi batas ketat pada penggunaan informasi pribadi. Menyadari bahwa kebanyakan orang tidak membaca *Daftar Federal,* GAO menyarankan cara yang lebih baik untuk menginformasikan kepada publik tentang basis data pemerintah dan kebijakan privasi. Dewan Informasi Keamanan dan Penasihat Privasi (dewan penasihat pemerintah) menunjukkan: “Undang-Undang Privasi tidak cukup mencakup penggunaan pemerintah dari database informasi pribadi yang dikompilasi secara komersial. Aturan tentang penggunaan pemerintah federal dari database komersial, dan bahkan penggunaan informasi yang diperoleh dari mesin pencari komersial, telah samar-samar dan kadang-kadang tidak ada. ”Dengan demikian, lembaga dapat melewati perlindungan dari Privacy Act dengan menggunakan database sektor swasta dan pencarian, daripada mengumpulkan informasi itu sendiri.

*Quis custodiet ipsos custodes? (Siapa yang akan menjaga penjaga itu sendiri?) -*

ContohJuvenal

**Contoh Basis Data : melacak mahasiswa**

Departemen Pendidikan AS mengusulkan untuk membuat database yang berisi catatan setiap siswa yang terdaftar di perguruan tinggi atau universitas di Amerika Serikat. Proposal tersebut akan membutuhkan perguruan tinggi dan universitas untuk menyediakan dan secara teratur memperbarui catatan termasuk nama masing-masing siswa, jenis kelamin, nomor Jaminan Sosial, jurusan, kursus yang diambil, kursus yang dilalui, gelar, pinjaman, dan beasiswa (publik dan swasta). Pemerintah akan menyimpan datanya tanpa batas. Departemen belum menerapkan proposal karena oposisi yang kuat. Pemerintah sudah memiliki basis data yang serupa, dan proposal untuk database pemerintah yang besar mengenai informasi pribadi muncul secara teratur. Kami membahas yang satu ini sebagai contoh untuk analisis; masalah dan pertanyaan yang kami ajukan di sini berlaku dalam banyak situasi lain.

Database siswa akan memiliki banyak kegunaan yang bermanfaat: Pemerintah federal menghabiskan miliaran dolar setiap tahun pada hibah federal dan pinjaman kepada siswa tetapi tidak memiliki cara yang baik untuk mengukur keberhasilan program-program ini. Apakah siswa yang mendapat bantuan sarjana? Jurusan apa yang mereka kejar? Database akan membantu mengevaluasi program bantuan siswa federal dan mungkin mengarah pada perbaikan dalam program. Database akan memberikan data yang lebih akurat tentang tingkat kelulusan dan biaya kuliah yang sebenarnya. Kemampuan untuk melacak jumlah perawat masa depan, insinyur, guru, dan sebagainya, dalam jalur pendidikan dapat membantu membentuk kebijakan imigrasi dan perencanaan bisnis dan ekonomi yang lebih baik.

Di sisi lain, pengumpulan begitu banyak detail tentang setiap siswa di satu tempat menghasilkan berbagai risiko privasi. Beberapa poin dalam daftar di Bagian 2.1.2 relevan di sini. Sangat mungkin bahwa pemerintah akan menemukan penggunaan baru untuk data yang bukan bagian dari proposal asli. Database semacam itu bisa menjadi target ideal bagi pencuri identitas. Kebocoran dari berbagai macam kemungkinan dan kemungkinan. Ada potensi penyalahgunaan oleh anggota staf yang memelihara data; misalnya, seseorang mungkin merilis catatan perguruan tinggi dari kandidat politik. Dan tidak diragukan lagi akan ada kesalahan dalam database. Jika departemen membatasi penggunaan data untuk analisis statistik umum, kesalahan mungkin tidak berdampak besar, tetapi untuk beberapa potensi penggunaan, kesalahan bisa sangat berbahaya. Beberapa pendidik khawatir bahwa kemungkinan hubungan antara database database dan sekolah umum (pada anak-anak di taman kanak-kanak sampai sekolah menengah) akan berkontribusi pada pelacakan "cradle-to-grave" dari masalah perilaku anak, masalah kesehatan dan keluarga, dan

sebagainya.

Penggunaan basis data yang direncanakan tidak termasuk mencari atau menyelidiki siswa yang melanggar hukum, tetapi itu akan menjadi sumber daya yang menggoda bagi lembaga penegak hukum. Hukum negara bagian Virginia mengharuskan perguruan tinggi untuk memberikan nama dan informasi pengenal lainnya untuk semua siswa yang mereka terima. Polisi negara bagian kemudian memeriksa apakah ada yang masuk dalam daftar pelanggar seks. Apa lagi yang bisa mereka periksa? Lembaga pemerintah lain mana yang ingin mendapat akses ke database mahasiswa federal? Akankah Departemen Pertahanan menggunakan database untuk merekrut militer? Risiko potensial apa yang muncul jika majikan mendapatkan akses? Semua kegunaan tersebut akan menjadi penggunaan sekunder, tanpa persetujuan

dari siswa.

Masuk akal bagi pemerintah untuk memantau keefektifan hibah dan pinjaman yang diberikan kepada mahasiswa. Oleh karena itu masuk akal untuk meminta data tentang kemajuan akademik dan kelulusan dari siswa yang menerima uang federal atau jaminan pinjaman. Tapi apa yang membenarkan menuntut data pada semua siswa lain? Untuk statistik dan perencanaan, pemerintah dapat melakukan survei sukarela, seperti halnya bisnis dan organisasi, tanpa paksaan pemerintah, harus dilakukan. Apakah manfaat dari pusat data cukup untuk tanggung jawab mendasar pemerintah untuk lebih besar daripada risiko dan untuk membenarkan program pelaporan wajib dari begitu banyak data pribadi pada setiap siswa?*\_*

*\_* Kritik terhadap proposal, termasuk banyak universitas, menunjukkan risiko dan biaya lain selain privasi. Perguruan tinggi takut

bahwa pengumpulan data akan menyebabkan peningkatan kontrol dan campur tangan federal dalam manajemen perguruan tinggi.

Persyaratan pelaporan akan membebankan biaya tinggi pada sekolah-sekolah. Seluruh proyek akan memiliki biaya tinggi untuk

pembayar pajak.

**Sensus Amerika Serikat (US)**

AS Konstitusi AS memberikan wewenang dan mengharuskan pemerintah untuk menghitung orang-orang di Amerika Serikat setiap 10 tahun, terutama untuk tujuan menentukan jumlah perwakilan Kongres yang akan dimiliki setiap negara. Antara 1870 dan 1880, populasi AS meningkat 26%. Pemerintah perlu sembilan tahun untuk memproses semua data dari sensus 1880. Selama tahun 1880-an, populasi meningkat 25% lagi. Jika Biro Sensus menggunakan metode yang sama, itu tidak akan menyelesaikan pemrosesan data dari sensus 1890 sampai setelah sensus 1900 dimulai. Herman Hollerith, seorang karyawan Biro Sensus, merancang dan membangun mesin pemroses kartu punch— tabulator, penyortir, dan mesin keypunch — untuk memproses data sensus. \* Mesin Hollerith melakukan penghitungan total populasi 1890 hanya dalam enam minggu — prestasi luar biasa pada saat itu. . Biro menyelesaikan sisa pemrosesan data sensus 1890 dalam tujuh tahun. Ini bisa dilakukan lebih cepat, tetapi mesin-mesin baru memungkinkan analisis yang canggih dan komprehensif dari data yang tidak mungkin dilakukan sebelumnya. Berikut ini adalah contoh awal dari teknologi komputasi yang memungkinkan peningkatan pemrosesan data dengan potensi efek yang baik dan buruk: penggunaan informasi yang lebih baik dan invasi privasi. Biro Sensus mengharuskan setiap orang untuk memberikan nama, jenis kelamin, usia, ras, dan hubungan dengan orang-orang yang tinggal bersama. Diperlukan tiga juta rumah tangga setahun untuk mengisi formulir yang lebih panjang yang berisi pertanyaan tentang riwayat perkawinan, leluhur, pendapatan, rincian tentang rumah seseorang, pendidikan, pekerjaan, cacat, pengeluaran, dan topik lainnya. Informasi sensus seharusnya bersifat rahasia. Undang-undang federal mengatakan bahwa “tidak ada informasi yang dilengkapi. . . digunakan untuk merugikan setiap responden atau orang lain kepada siapa informasi tersebut berhubungan. ” Selama Perang Dunia I, Biro Sensus memberikan nama dan alamat pemuda kepada pemerintah untuk membantu menemukan dan mengadili penolak draf. Selama Perang Dunia II, Biro Sensus membantu Departemen Kehakiman dalam menggunakan data dari sensus 1940 untuk menemukan warga negara AS keturunan Jepang; tentara mengumpulkan tentara Jepang-Amerika dan menempatkan mereka di kamp-kamp interniran. Dengan diperkenalkannya komputer elektronik dan kemajuan teknologi komputasi, menggunakan data "untuk merugikan setiap responden" lebih mudah. Beberapa kota menggunakan data sensus untuk menemukan keluarga miskin yang melanggar zonasi atau peraturan lain dengan menggandakan diri di perumahan keluarga tunggal. Mereka mengusir keluarga. Beberapa tahun setelah serangan teroris 9/11, atas permintaan Departemen Keamanan Tanah Air, Biro Sensus menyiapkan daftar yang menunjukkan jumlah orang leluhur Arab dalam berbagai kode pos di

seluruh Amerika Serikat. Seorang juru bicara pemerintah mengatakan mereka membutuhkan data untuk menentukan bandara mana yang harus memiliki tanda dalam bahasa Arab. Organisasi privasi dan kebebasan sipil skeptis.

\* Perusahaan Hollerith yang dibentuk untuk menjual mesin-mesinnya

kemudian menjadi IBM.

Ketika mempertimbangkan setiap sistem atau kebijakan baru untuk penggunaan data pribadi atau penambangan data oleh pemerintah, kita harus mengajukan banyak pertanyaan: Apakah informasi yang digunakan atau mengumpulkan akurat dan berguna? Akankah cara yang kurang mengganggu mencapai hasil yang sama? Akankah sistem tersebut menyusahkan orang biasa sementara menjadi mudah bagi penjahat dan teroris untuk menggagalkan? Seberapa signifikankah risiko bagi orang yang tidak bersalah? Apakah perlindungan privasi dibangun ke dalam teknologi dan ke dalam aturan yang mengontrol penggunaan?

**Memerangi terorisme**

Sebelum serangan teroris ke Amerika Serikat pada 11 September 2001, agen-agen penegak hukum melobi secara teratur untuk meningkatkan kekuatan yang bertentangan dengan privasi. Terkadang mereka mendapatkan apa yang mereka inginkan; terkadang mereka tidak melakukannya. Umumnya, orang-orang menolak gangguan privasi oleh pemerintah. Setelah serangan terhadap World Trade Center dan Pentagon, lebih banyak orang yang bersedia menerima penggunaan data pribadi dan bentuk pencarian dan pengawasan yang akan menghasilkan protes intens sebelumnya. Dua contoh adalah pencarian intrusif di bandara dan persyaratan Administrasi Keamanan Transportasi (TSA) bahwa maskapai penerbangan memberikan nama dan tanggal lahir setiap penumpang ke TSA sehingga dapat mencocokkan orang-orang dengan daftar pantauannya. Pada tahun 2012, pemerintah memperpanjang hingga lima tahun jumlah Pusat Nasional Kontraterorisme dapat menyimpan data pada orang Amerika yang tidak memiliki koneksi ke terorisme atau aktivitas kriminal.

Proposal untuk program penambangan data baru untuk menemukan teroris dan plot teroris terus muncul. Kami merangkum poin yang menarik Jeff Jonas dan JimHarper menyajikan tentang kesesuaian penambangan data untuk tujuan ini.56 Pemasar memanfaatkan banyak data mining. Mereka menghabiskan jutaan dolar untuk menganalisis data untuk menemukan orang-orang yang cenderung menjadi pelanggan. Seberapa besar kemungkinannya? Dalam pemasaran, tingkat respons beberapa persen dianggap cukup baik. Dengan kata lain, data mining yang mahal dan canggih memiliki tingkat false positive yang tinggi. Sebagian besar orang yang mengidentifikasi data mining sebagai pelanggan potensial tidak. Banyak orang yang ditargetkan akan menerima iklan, katalog, dan promosi penjualan yang tidak mereka inginkan. Email sampah dan iklan popup mengganggu orang, tetapi mereka tidak secara signifikan mengancam kebebasan sipil. Tingkat positif palsu yang tinggi dalam penambangan data untuk menemukan tersangka teroris. Penambangan data mungkin berguna untuk memilih teroris dari data konsumen, tetapi prosedur yang tepat.

**Mengurangi gangguan privasi untuk perjalanan udara**

Wisatawan akrab dengan mesin pemindai x-ray di bandara. Mesin-mesin menampilkan pada layar komputer gambar tubuh seseorang dan setiap senjata dan paket obat yang tersembunyi di bawah pakaian dan wig. American Civil Liberties Union (ACLU) mendeskripsikan pemindaian sebagai “virtual strip search.” Menanggapi keberatan yang kuat dari publik dan pendukung privasi, TSA memodifikasi perangkat lunak untuk menampilkan gambar garis generik dari sebuah badan, bukan x gambar -ray dari orang yang sebenarnya dipindai.57 Mengapa TSA tidak membangun fitur perlindungan privasi yang jelas ini di awal? Mungkin ada masalah teknis, tetapi mungkin mereka tidak melakukannya karena tidak ada undang-undang atau peraturan yang mengharuskan perlindungan privasi semacam itu. sangat penting untuk melindungi orang yang tidak bersalah tetapi salah pilih. Jonas dan Harper berpendapat bahwa metode lain untuk menemukan teroris lebih efektif biaya dan kurang mengancam privasi dan kebebasan sipil sejumlah besar orang.

### 2.4.2 Catatan Publik : Akses versus Privasi

Pemerintah memelihara "catatan publik," yaitu, catatan yang tersedia untuk masyarakat umum. Contohnya termasuk catatan kebangkrutan, catatan penangkapan, aplikasi lisensi pernikahan, proses perceraian, catatan kepemilikan properti (termasuk informasi hipotek), gaji pegawai pemerintah, dan surat wasiat. Ini sudah lama umum, tetapi pada umumnya mereka hanya tersedia di atas kertas di kantor-kantor pemerintah. Pengacara, detektif swasta, wartawan, broker real estate, tetangga, dan lainnya menggunakan catatan itu. Sekarang sangat mudah untuk mencari dan menelusuri file di Web, lebih banyak orang mengakses catatan publik untuk bersenang-senang, untuk penelitian, untuk tujuan pribadi yang valid — dan untuk tujuan yang dapat mengancam kedamaian, keselamatan, dan rahasia pribadi orang lain.

Catatan publik termasuk informasi sensitif seperti nomor Jaminan Sosial, tanggal lahir, dan alamat rumah. Daerah Maricopa di Arizona, county pertama yang menyimpan berbagai catatan publik lengkap di Web, memiliki tingkat pencurian identitas tertinggi di Amerika Serikat.58 Tentunya, informasi sensitif tertentu harus disembunyikan dari situs web catatan publik. Itu membutuhkan keputusan tentang jenis data apa yang harus dilindungi. Diperlukan revisi pada sistem perangkat lunak pemerintah untuk mencegah tampilan item yang ditentukan. Karena biaya dan kurangnya akuntabilitas, insentif dalam lembaga pemerintah untuk melakukan ini adalah lemah. Beberapa telah mengadopsi kebijakan untuk memblokir tampilan data sensitif dalam file yang diposting online, dan beberapa negara bagian memiliki undang-undang yang mewajibkannya. Beberapa perusahaan perangkat lunak menghasilkan perangkat lunak untuk tujuan ini, menggunakan berbagai teknik untuk mencari dokumen untuk data sensitif dan melindunginya. Sampai sistem baru — di mana keamanan semacam itu merupakan bagian dari desain dasar — ​​menggantikan ystem yang lebih tua, tambalan dan add-on, sementara bermanfaat, cenderung melewatkan banyak data sensitif.

Untuk mengilustrasikan lebih banyak isu tentang catatan publik dan solusi potensial, kami mendeskripsikan beberapa informasi khusus (kontribusi politik, informasi penerbangan untuk pesawat pribadi, dan laporan keuangan para hakim), kemudian mengajukan beberapa pertanyaan.

Komite kampanye politik harus melaporkan nama, alamat, majikan, dan jumlah donasi untuk setiap donor yang menyumbang lebih dari $ 100 kepada seorang calon presiden. Informasi ini tersedia untuk umum. Di masa lalu, terutama wartawan dan kampanye pesaing memeriksanya. Sekarang di Web dan mudah dicari. Siapa pun dapat mencari tahu apa yang kandidat tetangga, teman, karyawan, dan dukungan majikan mereka. Kami juga dapat menemukan alamat dari orang-orang terkemuka yang mungkin lebih suka menjaga kerahasiaan alamat mereka untuk melindungi kedamaian dan privasi mereka.

Pilot dari sekitar 10.000 pesawat perusahaan di Amerika Serikat mengajukan rencana penerbangan ketika mereka terbang. Beberapa bisnis telah menggabungkan informasi penerbangan ini, yang diperoleh dari database pemerintah, dengan catatan registrasi pesawat (juga catatan pemerintah umum) untuk memberikan layanan yang memberitahukan di mana pesawat tertentu berada, ke mana ia pergi, kapan akan tiba, dan seterusnya. Siapa yang menginginkan informasi ini? Pesaing dapat menggunakannya untuk menentukan dengan siapa eksekutif puncak dari perusahaan lain bertemu. Teroris bisa menggunakannya untuk melacak pergerakan target profil tinggi. Informasi itu tersedia sebelumnya, tetapi tidak begitu mudah dan anonim. Undang-undang federal mengharuskan hakim federal untuk mengajukan laporan pengungkapan keuangan.59 Publik dapat meninjau laporan-laporan ini untuk menentukan apakah seorang hakim tertentu mungkin memiliki konflik kepentingan dalam kasus tertentu. Laporannya tersedia dalam bentuk cetak tetapi tidak online. Ketika sebuah agensi berita online menggugat untuk membuat laporan tersedia secara online, hakim keberatan bahwa

informasi dalam laporan dapat mengungkapkan di mana anggota keluarga bekerja atau pergi ke sekolah, menempatkan mereka pada risiko dari terdakwa yang marah pada hakim. Pada akhirnya, laporan disediakan untuk diposkan online, dengan beberapa informasi sensitif dihapus.

     Perubahan dalam kemudahan akses informasi mengubah keseimbangan antara keuntungan dan kerugian dari pembuatan beberapa jenis data publik. Setiap kali akses berubah secara signifikan, kita harus mempertimbangkan kembali keputusan, kebijakan, dan hukum lama. Apakah manfaat mewajibkan pelaporan kontribusi politik kecil lebih besar daripada risiko privasi? Apakah manfaat dari membuat semua catatan kepemilikan properti publik lebih besar daripada risiko privasi? Mungkin. Intinya adalah bahwa pertanyaan semacam itu harus diangkat dan ditangani secara teratur.

Bagaimana seharusnya kita mengendalikan akses ke catatan publik yang sensitif? Di bawah aturan lama untuk laporan keuangan hakim, orang yang meminta akses harus menandatangani formulir yang mengungkapkan identitas mereka. Ini adalah aturan yang masuk akal. Informasi ini tersedia untuk umum, tetapi catatan tentang siapa yang mengaksesnya dapat menghalangi sebagian besar orang yang bermaksud melakukan bahaya. Bisakah kita menerapkan sistem serupa secara online? Teknologi untuk mengidentifikasi dan mengautentikasi online orang sedang berkembang, tetapi mereka belum cukup luas untuk digunakan oleh semua orang yang mengakses data publik yang sensitif di Web. Kami mungkin secara rutin menggunakannya di masa depan, tetapi itu menimbulkan pertanyaan lain: Bagaimana kita membedakan data yang memerlukan identifikasi dan tanda tangan untuk akses dari data publik harus bebas untuk melihat secara anonim, untuk melindungi privasi pemirsa?

### 2.4.3 Sistem ID Nasional

Di Amerika Serikat, sistem identifikasi nasional dimulai dengan kartu Jaminan Sosial pada tahun 1936. Dalam beberapa dekade terakhir, kekhawatiran tentang imigrasi ilegal dan terorisme memberikan dukungan terbesar untuk kartu ID nasional yang lebih canggih dan aman. Oposisi, berdasarkan kekhawatiran tentang privasi dan potensi penyalahgunaan (dan biaya dan masalah praktis), mencegah kemajuan signifikan pada berbagai proposal ID nasional yang dibuat oleh banyak lembaga pemerintah. Di bagian ini, kami meninjau nomor Jaminan Sosial, berbagai masalah tentang sistem ID nasional, dan UU ID NYATA, langkah besar untuk mengubah lisensi pengemudi menjadi kartu ID nasional.

**Nomor Jaminan Sosial**

Sejarah jumlah Jaminan Sosial (SSN) menggambarkan bagaimana penggunaan sistem identifikasi nasional tumbuh. Ketika SSN pertama kali muncul pada tahun 1936, mereka akan menggunakan program Jaminan Sosial secara eksklusif. Pemerintah meyakinkan masyarakat pada saat itu bahwa mereka tidak akan menggunakan angka untuk tujuan lain. Hanya beberapa tahun kemudian, pada tahun 1943, Presiden Roosevelt menandatangani sebuah perintah eksekutif yang mengharuskan agensi federal untuk menggunakan SSN untuk sistem catatan baru. Pada tahun 1961, IRS mulai menggunakannya sebagai nomor identifikasi pembayar pajak. Jadi majikan dan orang lain yang harus melapor ke IRS memerlukannya. Pada tahun 1976, departemen pajak, kesejahteraan, dan kendaraan bermotor negara bagian dan lokal menerima wewenang untuk menggunakan SSN. Undang-undang federal 1988 mengharuskan orang tua memberikan SSN mereka untuk mendapatkan akta kelahiran bagi seorang anak. Pada 1990-an, Federal Trade Commission mendorong biro kredit untuk menggunakan SSN. Undang-undang tahun 1996 mengharuskan negara mengumpulkan SSN untuk lisensi pekerjaan, surat nikah, dan jenis lisensi lainnya. Juga pada tahun 1996, Kongres mewajibkan agar semua surat izin mengemudi menampilkan SSN pengemudi, tetapi mencabut undang-undang itu beberapa tahun kemudian karena protes yang kuat. Meskipun pemerintah berjanji sebaliknya, SSN telah menjadi nomor identifikasi umum.

Kami menggunakan nomor Jaminan Sosial kami untuk identifikasi kredit, layanan keuangan, dan berbagai layanan lainnya, namun ketidakamanannya mengganggu privasi kami dan membuat kami terpidana penipuan dan pencurian identitas. Sebagai contoh, seorang guru bahasa Inggris paruh waktu di sebuah perguruan tinggi junior California menggunakan nomor Jaminan Sosial dari beberapa muridnya, yang disediakan di daftar kelasnya, untuk membuka rekening kartu kredit palsu. Karena SSN adalah pengidentifikasi dalam begitu banyak basis data, seseorang yang tahu nama Anda dan memiliki SSN Anda dapat, dengan berbagai tingkat kemudahan, mendapatkan akses ke pekerjaan dan riwayat penghasilan, laporan kredit, catatan mengemudi, dan data pribadi lainnya. SSN muncul di dokumen publik dan formulir lain yang tersedia secara terbuka. Akte properti, yang merupakan catatan publik (dan sekarang online), sering membutuhkan SSN. Selama beberapa dekade, SSN adalah nomor ID untuk mahasiswa dan fakultas di banyak universitas; angka-angka muncul di wajah kartu ID dan di daftar nama kelas. Negara bagian Virginia memasukkan SSN pada daftar pemilih yang diterbitkan sampai pengadilan federal memutuskan bahwa kebijakannya mengharuskan SSN untuk pendaftaran pemilih tidak konstitusional. Beberapa majikan menggunakan SSN sebagai pengidentifikasi dan menaruhnya di lencana atau memberikannya berdasarkan permintaan. Banyak perusahaan, rumah sakit, dan organisasi lain di mana kita mungkin berhutang tagihan meminta SSN kita untuk menjalankan pemeriksaan kredit. Beberapa orang secara rutin meminta SSN dan mencatatnya di file mereka, meskipun mereka tidak membutuhkannya.

Lebih dari 30 tahun yang lalu, Departemen Pertanian (USDA) mulai memasukkan SSN sebagai bagian dari nomor ID untuk petani yang menerima pinjaman atau hibah. Pada tahun 2007, USDA mengakui bahwa sejak tahun 1996 itu secara tidak sengaja memasukkan SSN dari lebih dari 35.000 petani di situs web di mana ia memposting rincian pinjaman.63 Contoh ini menggambarkan bagaimana praktik dimulai dengan baik sebelum Web terus beraksi. Ini juga menggambarkan pentingnya evaluasi yang cermat dan seksama atas keputusan untuk menempatkan materi di Web. Kemungkinan besar ada banyak contoh serupa yang belum diketahui oleh siapa pun.

SSN terlalu banyak tersedia untuk mengidentifikasi seseorang secara aman. Kartu jaminan sosial mudah dipalsukan, tetapi itu tidak masalah, karena mereka yang meminta nomor jarang menanyakan kartu dan hampir tidak pernah memverifikasi nomor. Administrasi Jaminan Sosial sendiri digunakan untuk mengeluarkan kartu tanpa verifikasi informasi yang diberikan oleh pemohon. Penjahat tidak banyak kesulitan menciptakan identitas palsu, sementara orang yang tidak bersalah dan jujur ​​menderita pengungkapan informasi pribadi, penangkapan, penipuan, penghancuran peringkat kredit mereka, dan sebagainya, karena masalah dengan SSN. Secara bertahap, pemerintah dan bisnis mulai mengenali risiko penggunaan yang sembrono dari SSN dan alasan mengapa kita tidak boleh menggunakannya secara luas. Ini bisa memakan waktu lama untuk membatalkan kerusakan yang telah digunakan secara luas pada privasi dan keamanan finansial.

**Sistem ID nasional baru**

*Tempat-tempat seperti Nazi Jerman, Uni Soviet, dan apartheid Afrika*

*Selatan semuanya memiliki sistem identifikasi yang sangat kuat. Benar,identifikasi*

*sistemtidak menyebabkan tirani, tetapi sistem identifikasi adalahyang sangat baik*

*sistem administrasiyang sering digunakan tirani.*

—Jim Harper, Direktur Studi Kebijakan Informasi, Cato Institute

Berbagai proposal kartu ID nasional dalam beberapa tahun terakhir akan membutuhkan kewarganegaraan, pekerjaan, kesehatan, pajak, keuangan, atau data lainnya, serta informasi biometrik seperti sidik jari atau scan retina, tergantung pada proposal khusus dan lembaga pemerintah yang mendukungnya. Dalam banyak proposal, kartu juga akan mengakses berbagai database untuk informasi tambahan.

Advokat sistem ID nasional menjelaskan beberapa manfaat: Anda akan membutuhkan kartu yang sebenarnya, bukan hanya nomor, untuk memverifikasi identitas. Kartu akan lebih sulit dipalsukan daripada kartu Jaminan Sosial. Seseorang hanya perlu membawa satu kartu, daripada kartu terpisah untuk berbagai layanan seperti yang kita lakukan sekarang. Otentikasi identitas akan membantu mengurangi penipuan baik dalam transaksi kartu kredit swasta dan dalam program tunjangan pemerintah. Penggunaan kartu ID untuk memverifikasi kelayakan kerja akan mencegah orang bekerja di Amerika Serikat secara ilegal. Penjahat dan teroris akan lebih mudah melacak dan mengidentifikasi.

Para penentang sistem ID nasional berpendapat bahwa mereka merupakan ancaman yang sangat besar terhadap kebebasan dan privasi. "Dokumen Anda, silakan" adalah permintaan yang terkait dengan negara polisi dan kediktatoran. Di Jerman dan Perancis, dokumen identifikasi termasuk agama orang itu, sehingga memudahkan bagi Nazi untuk menangkap dan menyingkirkan orang Yahudi. Di bawah undang-undang kelalaian yang terkenal di Afrika Selatan, orang membawa surat izin, atau kertas identifikasi, yang dikategorikan dengan ras dan dikendalikan di mana mereka dapat hidup dan bekerja. Kartu dengan chip atau strip magnetik tertanam dan sejumlah besar informasi pribadi yang dapat mereka bawa atau akses memiliki potensi lebih besar untuk penyalahgunaan. Sebagian besar orang tidak akan memiliki akses ke mesin yang membaca kartu. Dengan demikian, mereka tidak akan selalu tahu informasi apa yang mereka berikan kepada orang lain tentang diri mereka sendiri. Pencurian dan pemalsuan kartu akan mengurangi beberapa manfaat potensial. Peter Neumann dan Lauren Weinstein memperingatkan risiko yang muncul dari database dan kompleks komunikasi yang akan mendukung sistem kartu ID nasional: "Peluang untuk pengawasan yang terlalu bersemangat dan pelanggaran privasi serius hampir tidak terbatas, seperti kesempatan untuk menyamar, pencurian identitas, dan kejam rekayasa sosial dalam skala besar. ”

Seorang wanita di Kanada tidak bisa mendapatkan pengembalian pajak karena lembaga pajak bersikeras dia mati. Nomor identitasnya telah keliru dilaporkan sebagai pengganti ibunya ketika ibunya meninggal. Dia masih bisa mendapatkan pekerjaan baru, menarik uang dari rekening banknya, membayar sewa, mengirim email, dan pergi ke dokter ketika dia menyelesaikan masalah dengan agen pajak. Bagaimana jika database verifikasi pekerja terhubung ke database catatan kematian? Atau bagaimana jika kesalahan membatalkan satu kartu identitas yang diperlukan untuk semua transaksi ini? Seorang kritikus dari proposal untuk kartu identitas nasional di Australia menggambarkan kartu tersebut sebagai "lisensi untuk ada."

Undang-Undang ID NYATA berusaha untuk mengembangkan kartu identifikasi nasional yang aman dengan menetapkan standar federal untuk SIM (dan kartu ID yang dikeluarkan negara, untuk orang yang tidak memiliki SIM]. Lisensi harus memenuhi standar federal untuk digunakan untuk identifikasi oleh pemerintah federal. Tujuan tersebut termasuk keamanan bandara dan memasuki fasilitas federal. Implikasinya, mereka mungkin termasuk bekerja untuk pemerintah federal dan memperoleh keuntungan federal. Sangat mungkin bahwa pemerintah akan menambah banyak penggunaan baru, seperti yang dilakukan dengan nomor Jaminan Sosial. Bisnis dan pemerintah negara bagian dan lokal cenderung membutuhkan kartu ID yang disetujui pemerintah untuk banyak transaksi dan layanan. Pemerintah federal membayar setengah perawatan medis di Amerika Serikat (misalnya, Medicare, tunjangan bagi para veteran, dan sejumlah program yang didanai pemerintah federal). Tidak sulit untuk membayangkan membutuhkan SIM untuk layanan medis federal dan akhirnya menjadide

kartu ID medis nasionalfacto.

UU ID NYATA mensyaratkan bahwa, untuk mendapatkan SIM atau kartu ID yang disetujui pemerintah federal, setiap orang harus memberikan dokumentasi alamat, tanggal lahir, nomor Jaminan Sosial, dan status hukum di Amerika Serikat. Departemen kendaraan bermotor harus memverifikasi informasi setiap orang, sebagian dengan mengakses basis data federal seperti database Jaminan Sosial. Departemen harus memindai dokumen yang dikirimkan oleh pengemudi dan menyimpannya dalam bentuk yang dapat dipindahkan, setidaknya selama 10 tahun (membuat catatan kendaraan bermotor sebagai target yang diinginkan untuk pencuri identitas). Lisensi harus memenuhi berbagai persyaratan untuk mengurangi gangguan dan pemalsuan, dan mereka harus menyertakan foto orang itu dan informasi yang dapat dibaca mesin untuk ditentukan oleh Departemen Keamanan Dalam Negeri.

UU ID NYATA menempatkan beban verifikasi identitas pada individu dan departemen kendaraan bermotor negara. Kesalahan dalam basis data federal yang digunakan untuk verifikasi dapat mencegah orang untuk mendapatkan SIM mereka. Banyak negara keberatan dengan mandat dan biaya tinggi (diperkirakan dalam miliaran dolar). Lebih dari 20 negara mengeluarkan resolusi menolak untuk berpartisipasi. Warga di negara bagian tanpa izin mengemudi yang disetujui pemerintah federal dapat mengalami ketidaknyamanan yang serius. Kongres mengeluarkan ID NYATA pada tahun 2005, dan itu mulai berlaku pada tahun 2008. Departemen Keamanan Dalam Negeri memperpanjang batas waktu untuk kepatuhan beberapa kali, sementara beberapa anggota Kongres telah bekerja untuk mengubah atau mencabut ID NYATA. Ketika saya menulis ini, batas waktu tetap di masa depan, dan Kongres belum mencabut hukum.

Banyak negara Eropa dan Asia membutuhkan kartu tanda penduduk nasional. Rencana tidak populer untuk kartu ID nasional wajib mahal di Inggris terhenti ketika email tentang kelemahan rencana bocor dari kantor-kantor pemerintah. Pemerintah Jepang menerapkan sistem registrasi komputerisasi nasional yang mencakup pemberian nomor ID untuk setiap warga negara di negara tersebut. Sistem ini untuk keperluan pemerintah, awalnya dengan sekitar 100 aplikasi, tetapi akhirnya penggunaannya mungkin akan mencapai ribuan. Tujuannya adalah untuk menyederhanakan prosedur administrasi dan membuatnya lebih efisien. Pendukung privasi dan pengunjuk rasa mengeluhkan perlindungan privasi yang tidak memadai, potensi penyalahgunaan oleh pemerintah, dan kerentanan terhadap peretas. Pemerintah India sedang membangun basis data ID nasional untuk 1,2 miliar orang. Database akan mencakup foto setiap orang, sidik jari, pemindaian iris, tanggal lahir, dan informasi lainnya. Tujuannya termasuk meningkatkan penyediaan layanan pemerintah dan menangkap imigran gelap.

*Segera setelah Anda bersedia untuk menempatkan rumah Anda, kantor Anda, brankas Anda*

*, kunci sepeda Anda, kunci gym Anda, dan kunci meja Anda semua ke*

*satu dan minta pemerintah untuk mengeluarkan kunci itu, Anda akan baikbaik saja*

*-dengan ID Nasional. Namun hingga saat itu, kita perlu berpikir lebih dalam hal*

*diversifikasi sistem identifikasi.*

—Jim Harper, Direktur Studi Kebijakan Informasi, Cato Institute

## 2.5 Melindungi Privasi : Teknologi, Pasar, Hak, dan Hukum

### 2.5.1 Teknologi dan Pasar

Banyak individu, organisasi, dan bisnis membantu memenuhi permintaan privasi sampai tingkat tertentu: Posting pemrogram perorangan perangkat lunak perlindungan privasi gratis di Web. Pengusaha membangun perusahaan baru untuk memberikan perlindungan privasi berbasis teknologi. Bisnis besar menanggapi permintaan konsumen dan meningkatkan kebijakan dan layanan. Organisasi seperti Clearinghouse Hak Privasi menyediakan sumber informasi yang sangat baik. Organisasi aktivis seperti Pusat Informasi Privasi Elektronik menginformasikan kepada publik, mengajukan tuntutan hukum, dan mengadvokasi perlindungan privasi yang lebih baik.

Aplikasi teknologi baru sering dapat memecahkan masalah yang muncul sebagai efek samping dari teknologi. Segera setelah "teknisi" menjadi sadar akan penggunaan cookie oleh situs Web, mereka menulis cookie disablers dan mempostingnya di Web. Perangkat lunak untuk memblokir iklan pop-up muncul segera setelah munculnya iklan semacam itu. Orang-orang menemukan cara mencegah iklan agar tidak muncul di Gmail mereka dan memberi tahu dunia. Perusahaan menjual perangkat lunak untuk memindai spyware; beberapa versi gratis. Kita dapat menginstal add-on gratis ke browser kita yang memblokir pelacak aktivitas Web. Beberapa perusahaan menyediakan layanan, yang disebut anonymizers, dengan mana orang dapat menjelajahi Web secara anonim, tanpa meninggalkan catatan yang mengidentifikasi mereka atau komputer mereka. Beberapa mesin pencari tidak menyimpan permintaan pencarian pengguna dengan cara yang memungkinkan menghubungkan mereka bersama untuk satu orang.68 Perusahaan menawarkan produk dan layanan untuk mencegah penerusan, penyalinan, atau pencetakan email. (Pengacara adalah salah satu pelanggan utama.) Ada layanan yang sepenuhnya menghapus email atau pesan teks (pada telepon pengirim dan penerima) setelah jangka waktu yang ditentukan pengguna. Mereka dapat membantu dokter, yang harus mengikuti peraturan privasi medis yang sangat ketat.

Beberapa sistem pelacakan untuk laptop, tablet, dan telepon termasuk fitur yang memungkinkan pemilik laptop yang dicuri atau hilang untuk mengenkripsi, mengambil, dan / atau menghapus file dari jarak jauh.

Ini adalah contoh yang sangat sedikit dari banyak produk dan aplikasi teknologi yang melindungi privasi. Mereka mengilustrasikan bahwa individu, bisnis, dan organisasi cepat merespon dan menyediakan alat perlindungan privasi. Mereka memiliki kelebihan dan kekurangan; mereka tidak menyelesaikan semua masalah. Mempelajari, menginstal, dan menggunakan alat privasi mungkin menakutkan bagi pengguna nonteknis dan kurang terdidik — sebagian besar masyarakat — maka pentingnya merancang sistem dengan perlindungan privasi, membangun fitur perlindungan, dan memiliki kebijakan perlindungan privasi.

**Enkripsi**

*Kriptografi adalah seni dan ilmu menyembunyikan data di depan mata.*

—Larry Loen

Adalah mungkin untuk mencegat email dan data transit di Internet dan untuk memilih transmisi nirkabel dari udara. Seseorang yang mencuri komputer atau hacks menjadi satu dapat melihat file di dalamnya. Kebanyakan orang yang menguping oleh warga negara adalah ilegal. Meretas dan mencuri laptop adalah kejahatan. Undang-undang menetapkan hukuman bagi pelanggar ketika tertangkap dan dihukum, tetapi kita juga dapat menggunakan teknologi untuk melindungi diri kita sendiri.

Enkripsi adalah teknologi, sering diimplementasikan dalam perangkat lunak, yang mengubah data menjadi bentuk yang tidak berarti bagi siapa saja yang mungkin mencegat atau melihatnya. Data bisa berupa email, rencana bisnis, nomor kartu kredit, gambar, catatan medis, riwayat lokasi ponsel, dan sebagainya. Perangkat lunak di situs penerima (atau di komputer sendiri) menerjemahkan data terenkripsi sehingga penerima atau pemilik dapat melihat pesan atau file. Perangkat lunak secara rutin mengenkripsi nomor kartu kredit ketika kami mengirimnya ke pedagang daring. Orang sering tidak menyadari bahwa mereka menggunakan enkripsi. Perangkat lunak menanganinya secara otomatis.

Banyak ahli privasi dan keamanan profesional melihat enkripsi sebagai metode teknis yang paling penting untuk memastikan privasi pesan dan data yang dikirim melalui jaringan komputer. Enkripsi juga melindungi informasi yang disimpan dari penyusup dan pelanggaran oleh karyawan. Ini adalah perlindungan terbaik untuk data pada laptop dan perangkat penyimpanan data kecil lainnya yang dibawa di luar kantor.

Enkripsi umumnya mencakup skema pengkodean, atau algoritme kriptografi, dan rangkaian karakter tertentu (misalnya, angka atau huruf), yang disebut *kunci*, yang digunakan oleh algoritme. Dengan menggunakan alat-alat matematika dan komputer yang kuat, kadang-kadang mungkin untuk "memecahkan" skema enkripsi — yaitu, untuk memecahkan kode pesan terenkripsi atau file tanpa kunci rahasia.

Teknologi enkripsi modern memiliki fleksibilitas dan berbagai aplikasi di luar perlindungan data. Misalnya, digunakan untuk membuat tanda tangan digital, metode otentikasi, dan uang digital. Teknologi tanda tangan digital memungkinkan kita untuk "menandatangani" dokumen secara online, menghemat waktu dan kertas untuk aplikasi pinjaman, kontrak bisnis, dan sebagainya. Dalam satu aplikasi otentikasi khusus, yang bertujuan untuk mengurangi risiko akses tidak sah ke informasi medis online, American Medical Association mengeluarkan kredensial digital kepada dokter yang dapat diverifikasi oleh situs web laboratorium ketika dokter berkunjung untuk mendapatkan hasil tes pasien. Mungkin ada ribuan aplikasi teknologi ini.

Kas digital dan metode transaksi perlindungan privasi berbasis enkripsi lainnya dapat memungkinkan kita melakukan transaksi keuangan aman secara elektronik tanpa penjual mendapatkan kartu kredit atau nomor rekening cek dari pembeli. Mereka menggabungkan kenyamanan pembelian kartu kredit dengan anonimitas uang tunai. Dengan skema seperti itu, tidak mudah untuk menghubungkan catatan dari berbagai transaksi untuk membentuk profil atau dokumen konsumen. Teknik-teknik ini dapat memberikan perlindungan privasi bagi konsumen berkenaan dengan organisasi yang dia berinteraksi dengan dan perlindungan untuk organisasi terhadap pemalsuan, pemeriksaan buruk, dan penipuan kartu kredit. Namun, transaksi tunai menyulitkan pemerintah untuk mendeteksi dan mengadili orang-orang yang "mencuci" uang yang diperoleh dalam kegiatan ilegal, mendapatkan uang mereka tidak melaporkan kepada otoritas pajak, atau mentransfer atau menghabiskan uang untuk tujuan kriminal. Dengan demikian, sebagian besar pemerintah akan menentang dan mungkin melarang sistem uang digital anonim yang sesungguhnya. Beberapa sistem uang digital termasuk ketentuan untuk penegakan hukum dan pengumpulan pajak. Potensi penggunaan ilegal dari uang tunai digital telah lama dimungkinkan dengan uang nyata. Hanya dalam beberapa dekade terakhir, dengan meningkatnya penggunaan cek dan kartu kredit, kami kehilangan privasi yang kami miliki dari pemasar dan pemerintah ketika kami menggunakan uang tunai untuk sebagian besar transaksi.

*Teknologi anonimitas dan kriptografi mungkin satu-satunya cara*

*untuk melindungi privasi.*

—Nadine Strossen, presidenKebebasan Sipil Amerika

**Kebijakan - Kebijakan untuk melindungi data pribadi**

Bisnis, organisasi, dan lembaga pemerintah yang mengumpulkan dan menyimpan data pribadi memiliki tanggung jawab etis (dan dalam banyak kasus yang sah) untuk melindunginya dari penyalahgunaan. Pemegang data yang bertanggung jawab harus mengantisipasi risiko dan mempersiapkannya. Mereka harus terus memperbarui kebijakan keamanan untuk mencakup teknologi baru dan potensi ancaman baru.

**Kebijakan Enkripsi**

Selama berabad-abad sebelum Internet, pemerintah, agen militer mereka, dan mata-mata mereka adalah pengguna utama kode. Selama beberapa dekade, sebagian besar cryptographers di Amerika Serikat bekerja untuk National Security Agency (NSA). NSA hampir pasti dapat memecahkan hampir semua kode yang digunakan hingga awal 1970-an.71 NSA bekerja keras untuk menjaga segala sesuatu tentang rahasia enkripsi. Pada tahun 1970-an, terobosan sektor swasta yang disebut kriptografi kunci publik menghasilkan enkripsi yang relatif mudah digunakan dan sangat sulit untuk dipecahkan. Menjaga enkripsi sebagai alat eksklusif pemerintah dan mata-mata tidak lagi menjadi pilihan. Sepanjang tahun 1990-an, ketika orang mulai menggunakan enkripsi untuk email dan tujuan lain, pemerintah AS memerangi komunitas internet dan pendukung privasi untuk membatasi ketersediaan enkripsi aman (yaitu enkripsi yang sangat sulit dan mahal untuk memecahkannya sehingga tidak praktis untuk melakukannya.) Ini mempertahankan kebijakan mahal dan akhirnya sia-sia melarang ekspor perangkat lunak enkripsi yang kuat. Pemerintah menafsirkan apa pun yang diposting di Internet sebagaimana diekspor secara efektif. Dengan demikian, bahkan peneliti yang memasang algoritma enkripsi di Net menghadapi kemungkinan penuntutan. Pemerintah berpendapat bahwa larangan ekspor diperlukan untuk menjaga enkripsi yang kuat dari teroris dan pemerintah musuh. Kebijakan AS anehnya ketinggalan zaman. Skema enkripsi yang lebih kuat tersedia di situs-situs Internet di seluruh dunia. Dewan Riset Nasional (afiliasi penelitian National Academy of Sciences) sangat mendukung penggunaan enkripsi yang kuat dan pelonggaran kontrol ekspor. Dikatakan bahwa enkripsi yang kuat memberikan perlindungan yang meningkat terhadap peretas, pencuri, dan teroris yang mengancam infrastruktur ekonomi, energi, dan transportasi kita. Kebutuhan akan enkripsi yang kuat dalam perdagangan elektronik juga menjadi semakin jelas. Bersamaan dengan larangan ekspor enkripsi yang kuat, pemerintah berusaha untuk memastikan aksesnya ke kunci enkripsi (atau ke konten terenkripsi pesan terenkripsi) untuk enkripsi yang digunakan di Amerika Serikat. Pedofilia dan penganiaya anak mengenkripsi pornografi anak di komputer mereka. Penjahat lainnya mengenkripsi email dan file untuk menyembunyikan isinya dari agen penegak hukum. FBI mendukung RUU yang membutuhkan celah, atau "backdoor," di semua produk enkripsi yang dibuat, dijual, atau digunakan di Amerika Serikat untuk memungkinkan dekripsi segera data terenkripsi pada saat diterimanya perintah pengadilan.73 FBI berpendapat bahwa wewenang untuk mencegat panggilan telepon atau email atau merebut komputer tidak berarti apa-apa jika agen tidak dapat membaca apa yang mereka sita. Para ahli teknis berpendapat bahwa hukum seperti itu akan sangat sulit untuk diimplementasikan karena enkripsi sekarang menjadi bagian dari browser Web dan banyak alat komputasi umum lainnya. Implementasi mekanisme dekripsi segera akan mengancam privasi dan sangat melemahkan keamanan perdagangan elektronik dan komunikasi. Selama waktu yang sama, pengadilan mempertimbangkan tantangan hukum terhadap pembatasan ekspor berdasarkan Amandemen Pertama. Pertanyaannya adalah apakah algoritma kriptografi, dan program komputer pada umumnya, adalah pidato dan karenanya dilindungi oleh Amandemen Pertama. Pemerintah berpendapat bahwa perangkat lunak tidak berbicara dan bahwa pengendalian kriptografi adalah masalah keamanan nasional, bukan masalah kebebasan berbicara. Hakim federal yang mendengar kasus itu berpikir sebaliknya. Dia berkata: Pengadilan ini tidak dapat menemukan perbedaan yang berarti antara bahasa komputer. . . dan Jerman atau Prancis. . . . Seperti musik dan persamaan matematika, bahasa komputer hanya itu, bahasa, dan berkomunikasi informasi baik ke komputer atau kepada mereka yang bisa membacanya. . . . Untuk keperluan analisis Amandemen Pertama, pengadilan ini menemukan bahwa kode sumber adalah pidato. Pemerintah AS menghapus hampir semua pembatasan ekspor pada enkripsi pada tahun 2000. Kongres tidak mengeluarkan undang-undang yang mengharuskan semua enkripsi memiliki mekanisme untuk akses penegakan hukum. Di antara ribuan penyadapan yang disetujui untuk penyelidikan kriminal pada tahun 2010, agen penegak hukum menemukan enkripsi hanya enam kali dan dapat memperoleh teks biasa dari pesan-pesan tersebut.

Pengusaha harus melatih mereka yang membawa data pribadi tentang risiko dan langkah-langkah pengamanan.

Basis data yang dirancang dengan baik untuk informasi sensitif mencakup beberapa fitur untuk melindungi kebocoran, penyusup, dan akses karyawan yang tidak sah. Setiap orang dengan akses resmi ke sistem harus memiliki pengenal unik dan kata sandi. Suatu sistem dapat membatasi pengguna dari melakukan operasi tertentu, seperti menulis atau menghapus, pada beberapa file. User ID dapat dikodekan sehingga mereka memberikan akses ke hanya bagian-bagian tertentu dari suatu record. Misalnya, petugas penagihan di rumah sakit tidak memerlukan akses ke hasil tes laboratorium pasien. Sistem komputer melacak informasi tentang setiap akses, termasuk ID orang yang melihat catatan dan informasi tertentu yang dilihat atau diubah. Ini adalah *jejak audit* yang nantinya dapat membantu melacak aktivitas yang tidak sah. Pengetahuan bahwa suatu sistem mengandung ketentuan seperti itu akan mencegah banyak pelanggaran privasi.

Basis data dengan informasi konsumen, catatan aktivitas-Web, atau data lokasi ponsel adalah aset berharga yang memberikan keunggulan kompetitif bagi bisnis. Pemilik data tersebut memiliki kepentingan dalam mencegah kebocoran dan distribusi tidak terbatas. Itu termasuk memberikan keamanan untuk data dan mengembangkan mode operasi yang mengurangi kerugian. Jadi, misalnya, milis biasanya tidak dijual; mereka "disewa." Penyewa tidak menerima salinan (elektronik atau sebaliknya). Perusahaan khusus melakukan pengiriman surat. Risiko penyalinan tidak sah dengan demikian dibatasi untuk sejumlah kecil perusahaan yang reputasinya untuk kejujuran dan keamanan adalah penting untuk bisnis mereka. Aplikasi lain juga menggunakan ide pihak ketiga yang dipercaya untuk memproses data rahasia. Beberapa agen penyewaan mobil mengakses layanan pihak ketiga untuk memeriksa catatan mengemudi pelanggan potensial. Layanan memeriksa catatan departemen kendaraan bermotor; perusahaan rental mobil tidak melihat catatan pengemudi

.

Operator situs web membayar ribuan, terkadang jutaan dolar kepada perusahaan yang melakukan *audit privasi*. Auditor privasi memeriksa kebocoran informasi, meninjau kebijakan privasi perusahaan dan kepatuhannya terhadap kebijakan itu, mengevaluasi peringatan dan penjelasan di situsnya yang memperingatkan pengunjung ketika situs meminta data sensitif, dan sebagainya. Ratusan bisnis besar memiliki posisi yang disebut *chief privacy officer*. Orang ini memandu kebijakan privasi perusahaan. Sama seperti Asosiasi Mobil Amerika menilai hotel, Better Business Bureau, dan organisasi serupa menawarkan persetujuan, perusahaan ikon yang mematuhi standar privasi mereka dapat memposting di situs web.

Perusahaan besar menggunakan pengaruh ekonomi mereka untuk meningkatkan privasi konsumen. IBM dan Microsoft menghapus iklan Internet dari situs web yang tidak memposting kebijakan privasi yang jelas. Wal Disney Company dan Infoseek Corporation melakukan hal yang sama dan, di samping itu, berhenti menerima iklan di situs web mereka dari situs yang tidak memposting kebijakan privasi. Asosiasi Pemasaran Langsung mengadopsi kebijakan yang mewajibkan perusahaan anggotanya untuk menginformasikan kepada konsumen ketika mereka akan berbagi informasi pribadi dengan pemasar lain dan memberi orang pilihan menyisih. Banyak perusahaan setuju untuk membatasi ketersediaan informasi konsumen yang sensitif, termasuk nomor telepon yang tidak terdaftar, sejarah mengemudi, dan semua informasi tentang anak-anak.

Di sana terus, tentu saja, menjadi banyak bisnis tanpa kebijakan privasi yang kuat, serta banyak yang tidak mengikuti kebijakan yang mereka nyatakan sendiri. Contoh yang dijelaskan di sini mewakili tren, bukan utopia privasi. Mereka menyarankan tindakan yang dapat diambil oleh perusahaan yang bertanggung jawab. Karena beberapa masalah ditangani, masalah baru akan terus muncul.

### 2.5.2 Hak dan Hukum

Di Bagian 2.2, kami mempertimbangkan beberapa aspek hukum dan prinsip Perubahan Keempat terkait dengan perlindungan privasi. Amandemen Keempat melindungi hak negatif (kebebasan) terhadap intrusi dan campur tangan pemerintah. Bagian ini berfokus terutama pada diskusi tentang prinsip-prinsip yang berkaitan dengan hak dan perlindungan hukum untuk data pribadi yang dikumpulkan atau digunakan oleh orang lain, bisnis, dan organisasi.

Kami memisahkan pemulihan hukum dari solusi teknis, manajemen, dan pasar karena mereka pada dasarnya berbeda. Yang terakhir bersifat sukarela dan bervariasi. Orang atau bisnis yang berbeda dapat memilih di antara mereka. Hukum, di sisi lain, ditegakkan oleh denda, hukuman penjara, dan hukuman lainnya. Jadi, kita harus memeriksa dasar hukum dengan lebih hati-hati. Privasi adalah kondisi atau keadaan yang kita bisa hadapi, seperti kesehatan yang baik atau keamanan finansial. Sejauh mana kita harus memiliki hak legal untuk itu? Apakah itu hak negatif atau hak positif (dalam arti Bagian 1.4.2)? Seberapa jauh hukum harus pergi, dan apa yang harus diserahkan kepada interaksi sukarela pasar, upaya pendidikan kelompok kepentingan umum, pilihan dan tanggung jawab konsumen, Dan seterusnya?

Hingga akhir abad ke-19, pengadilan mengambil keputusan hukum yang mendukung privasi dalam kegiatan sosial dan bisnis tentang hak milik dan kontrak. Tidak ada pengakuan hak independen atas privasi. Pada tahun 1890, sebuah artikel penting yang disebut "The Right of Privacy," oleh SamuelWarren dan Louis Brandeis76 (kemudian Hakim Agung), berpendapat bahwa privasi berbeda dari hak lain dan membutuhkan perlindungan lebih. Judith Jarvis Thomson, seorang filsuf MIT, berpendapat bahwa pandangan lama lebih akurat, bahwa dalam semua kasus di mana pelanggaran privasi adalah pelanggaran hak seseorang, pelanggaran itu adalah hak yang berbeda dari privasi.77 Kami menyajikan beberapa klaim dan argumen dari makalah ini. Kemudian kami mempertimbangkan berbagai ide dan perspektif lain tentang hukum untuk melindungi privasi.

Salah satu tujuan dari bagian ini adalah untuk menunjukkan jenis-jenis analisis yang dilakukan oleh para filsuf, sarjana hukum, dan para ekonom dalam mencoba untuk menjelaskan prinsip-prinsip dasar. Lain adalah untuk menekankan pentingnya prinsip, bekerja di luar kerangka teoritis di mana untuk membuat keputusan tentang isu-isu dan kasus-kasus tertentu.

**Warren and Brandeis : The inviolate personality**

Target utama kritik dalam artikel 1890 Warren and Brandeis adalah surat kabar, terutama kolom gosip. Warren dan Brandeis dengan keras mengkritik pers karena “melangkahi. . . batas-batas kepatutan dan kesopanan. ”Jenis-jenis informasi yang paling mempedulikan mereka adalah penampilan pribadi, pernyataan, tindakan, dan hubungan interpersonal (perkawinan, keluarga, dan lain-lain).78 Warren dan Brandeis mengambil posisi bahwa orang memiliki hak untuk melarang publikasi fakta tentang diri mereka sendiri dan foto-foto diri mereka sendiri.Warren dan Brandeis berpendapat bahwa, misalnya, jika seseorang menulis surat di mana dia mengatakan dia memiliki argumen sengit dengan istrinya , penerima surat tidak dapat mempublikasikan informasi itu. Mereka mendasarkan klaim ini pada hak milik atau hak lain selain

privasi. Ini adalah bagian dari hak untuk dibiarkan sendiri. Warren dan Brandeis mendasarkan pembelaan mereka terhadap hak privasi, dalam frasa mereka yang sering dikutip, prinsip "kepribadian yang tidak berkepentingan."

Hukum terhadap kesalahan lain (seperti fitnah, fitnah, pencemaran nama baik, pelanggaran hak cipta, pelanggaran hak milik, dan pelanggaran kontrak) dapat mengatasi beberapa pelanggaran privasi, tetapiWarren dan Brandeis berpendapat bahwa masih banyak pelanggaran privasi yang tidak dipenuhi oleh undang-undang lainnya. Misalnya, publikasi informasi pribadi atau bisnis dapat merupakan pelanggaran kontrak (eksplisit atau tersirat), tetapi ada banyak kasus di mana orang yang mengungkapkan informasi tidak memiliki kontrak dengan korban. Orang itu tidak melanggar kontrak tetapi melanggar privasi korban. Undang-undang pencemaran nama baik, fitnah, dan pencemaran nama baik melindungi kita ketika seseorang menyebarkan desas-desus palsu dan merusak tentang kita, tetapi mereka tidak berlaku untuk informasi pribadi sejati yang pemaparannya membuat kita tidak nyaman.Warren dan Brandeis mengatakan privasi berbeda dan membutuhkan perlindungannya sendiri. Mereka mengizinkan pengecualian untuk publikasi informasi kepentingan umum (berita), digunakan dalam situasi terbatas ketika informasi menyangkut kepentingan orang lain, dan publikasi lisan. (Mereka menulis sebelum radio dan televisi, sehingga publikasi lisan berarti penonton yang sangat terbatas.)

**Judith Jarvis Thomson: Apakah ada hak untuk privasi?**

Judith Jarvis Thomson berpendapat sudut pandang sebaliknya. Dia sampai pada intinya setelah memeriksa beberapa skenario.

Misalkan Anda memiliki salinan majalah. Hak milik Anda termasuk hak untuk menolak mengizinkan orang lain membaca, menghancurkan, atau bahkan melihat majalah Anda. Jika seseorang melakukan sesuatu pada majalah Anda yang tidak Anda izinkan, orang itu melanggar hak milik Anda. Misalnya, jika seseorang menggunakan teropong untuk melihat majalah Anda dari gedung tetangga, orang itu melanggar hak Anda untuk mengecualikan orang lain agar tidak melihatnya. Tidak masalah apakah majalah itu adalah majalah berita biasa (bukan masalah privasi yang sensitif) atau majalah lain yang Anda tidak ingin orang tahu Anda baca. Hak yang dilanggar adalah hak milik Anda.

Anda dapat mengesampingkan hak milik Anda, secara sengaja atau tidak sengaja. Jika Anda linglung meninggalkan majalah di bangku taman, seseorang bisa menerimanya. Jika Anda meninggalkannya di meja kopi ketika Anda memiliki tamu di rumah Anda, seseorang bisa melihatnya. Jika Anda membaca majalah porno di bus, dan seseorang melihat Anda dan memberi tahu orang lain bahwa Anda membaca majalah kotor, orang itu tidak melanggar hak Anda. Orang itu mungkin melakukan sesuatu yang tidak sopan, tidak ramah, atau kejam, tetapi bukan sesuatu yang melanggar hak.

Hak kami untuk orang dan tubuh kami termasuk hak untuk memutuskan kepada siapa kami menunjukkan berbagai bagian tubuh kami. Dengan berkeliling di depan umum, sebagian besar dari kita mengabaikan hak kita untuk mencegah orang lain melihat wajah kita. Ketika seorang wanita Muslim menutupi wajahnya, dia menggunakan haknya untuk membuat orang lain tidak melihatnya. Jika seseorang menggunakan teropong untuk memata-matai kita di rumah di kamar mandi, mereka melanggar hak kita untuk orang kita.

Jika seseorang memukul Anda untuk mendapatkan beberapa informasi, pemukul itu melanggar hak Anda untuk bebas dari gangguan fisik yang dilakukan oleh orang lain. Jika informasinya adalah waktu, privasi tidak dipermasalahkan. Jika informasinya lebih pribadi, maka mereka telah mengganggu privasi Anda, tetapi hak yang dilanggar adalah hak Anda untuk bebas dari serangan. Di sisi lain, jika seseorang dengan damai bertanya dengan siapa Anda tinggal atau pandangan politik Anda, mereka tidak melanggar hak. Jika Anda memilih untuk menjawab dan tidak membuat perjanjian kerahasiaan, orang tersebut tidak melanggar hak Anda dengan mengulangi informasi itu kepada orang lain, meskipun itu mungkin tidak bijaksana untuk melakukannya. Namun, jika orang tersebut setuju untuk tidak mengulangi informasi, tetapi kemudian, tidak masalah apakah informasi itu sensitif atau tidak; orang itu melanggar perjanjian kerahasiaan.

Dalam contoh-contoh ini, tidak ada pelanggaran privasi tanpa pelanggaran terhadap hak lain, seperti hak untuk mengontrol properti kami atau orang kami, hak untuk bebas dari serangan kekerasan, atau hak untuk membentuk kontrak (dan mengharapkan mereka untuk menjadi diberlakukan). Thomson menyimpulkan, “Saya menyarankan ini adalah alat heuristik yang berguna dalam kasus pelanggaran hak privasi yang dituduhkan untuk menanyakan apakah tindakan tersebut merupakan pelanggaran hak lainnya, dan jika bukan apakah tindakan tersebut benar-benar melanggar hak di semua. ”

**Kritik terhadap Warren dan Brandeis dan Thomson**

Kritik terhadap posisi Warren dan Brandeis80 berpendapat bahwa itu tidak memberikan prinsip atau definisi yang bisa diterapkan untuk menyimpulkan bahwa pelanggaran hak privasi terjadi. Gagasan privasi mereka terlalu luas. Itu bertentangan dengan kebebasan pers. Tampaknya hampir semua penyebutan orang yang tidak sah merupakan pelanggaran hak orang tersebut.

Kritik Thomson menyajikan contoh pelanggaran hak privasi (bukan hanya keinginan untuk privasi), tetapi tidak ada hak lain. Sebagian orang memandang pengertian Thomson tentang hak atas orang kita sebagai samar atau terlalu luas. Contohnya mungkin (atau mungkin tidak) menjadi argumen yang meyakinkan untuk tesis yang mempertimbangkan hak-hak lain dapat menyelesaikan pertanyaan privasi, tetapi tidak ada sejumlah contoh yang dapat membuktikan tesis seperti itu.

Tidak ada artikel yang langsung menyanggah yang lain. Penekanan mereka berbeda. Warren dan Brandeis fokus pada penggunaan informasi (publikasi). Thomson berfokus pada bagaimana ia diperoleh. Perbedaan ini terkadang mendasari perbedaan dalam argumen oleh mereka yang mengadvokasi peraturan hukum yang kuat tentang penggunaan data pribadi dan mereka yang menganjurkan lebih banyak

ketergantungan pada solusi teknis, kontrak, dan pasar.

**Menerapkan teori**

Bagaimana argumen teoritis berlaku untuk privasi dan data pribadi hari ini?

Di seluruh Washington dan Brandeis, tindakan yang tidak pantas adalah publikasi informasi pribadi — penyebarannya yang luas dan bersifat publik. Banyak putusan pengadilan sejak munculnya artikel mereka telah mengambil sudut pandang ini.81 Jika seseorang menerbitkan informasi dari database konsumen (dicetak atau dengan mempublikasikannya di Web), itu akan melanggar gagasan privasi Warren dan Brandeis. Seseorang mungkin memenangkan kasus jika seseorang menerbitkan profil konsumennya. Namun publikasi yang disengaja bukanlah perhatian utama dalam konteks database konsumen saat ini, pemantauan aktivitas Web, pelacakan lokasi, dan sebagainya. Jumlah informasi pribadi yang dikumpulkan saat ini mungkin akan mengejutkan Warren dan Brandeis, tetapi artikel mereka memungkinkan pengungkapan informasi pribadi kepada orang-orang yang memiliki minat terhadapnya. Implikasinya, mereka tidak menghalangi, misalnya, pengungkapan catatan mengemudi seseorang ke perusahaan rental mobil dari mana dia ingin menyewa mobil. Demikian pula, tampaknya Warren dan Brandeis tidak akan menentang pengungkapan informasi tentang apakah seseorang menghisap rokok ke perusahaan asuransi jiwa dari siapa orang tersebut mencoba membeli asuransi. Pandangan mereka tidak mengesampingkan penggunaan informasi konsumen (yang tidak dipublikasikan) untuk pemasaran yang ditargetkan, meskipun mereka mungkin akan menolaknya.

Konten jejaring sosial mungkin akan mengejutkan dan mengagetkan Warren dan Brandeis. Posisi mereka akan sangat membatasi pembagian foto yang mencakup orang lain dan lokasi serta kegiatan teman-teman.

Aspek penting dari kedua kertas Warren dan Brandeis dan kertas Thomson adalah persetujuan. Mereka tidak melihat pelanggaran privasi jika seseorang menyetujui pengumpulan dan penggunaan informasi.

**Transaksi**

Kami memiliki teka-teki lain untuk dipertimbangkan: bagaimana menerapkan filosofi dan pengertian hukum tentang privasi pada transaksi, yang secara otomatis melibatkan lebih dari satu orang. Skenario berikut ini akan mengilustrasikan masalah.

Suatu hari di komunitas pertanian kecil di Friendlyville, Joe membeli lima pon kentang dari Maria, yang menjualnya lima pon kentang. (Saya jelaskan transaksi dengan cara yang berulang-ulang ini untuk menekankan bahwa ada dua orang yang terlibat dan dua sisi transaksi.)

Baik Joe atau Maria mungkin lebih memilih transaksi untuk tetap dirahasiakan. Kegagalan tanaman kentangnya sendiri mungkin mempermalukan Joe. Atau Joe mungkin tidak populer di Friendlyville, dan Maria takut orang kota akan marah padanya karena menjual kepadanya. Either way, kita tidak mungkin menganggapnya sebagai pelanggaran hak-hak lain jikaMaria atau Joe berbicara tentang pembelian atau penjualan kentang kepada orang lain di kota. Tetapi anggaplah Joe meminta kerahasiaan sebagai bagian dari transaksi. Maria memiliki tiga pilihan. (1) Dia setuju. (2) Dia bisa mengatakan tidak; dia mungkin ingin memberi tahu orang-orang bahwa dia menjual kentang kepada Joe. (3) Dia dapat setuju untuk merahasiakan penjualan jika Joe membayar harga yang lebih tinggi. Dalam dua kasus terakhir, Joe dapat memutuskan apakah akan membeli kentang. Di sisi lain, jika Maria meminta kerahasiaan sebagai bagian dari transaksi, Joe memiliki tiga opsi. (1) Dia bisa setuju. (2) Ia bisa berkata tidak; dia mungkin ingin memberi tahu orang-orang bahwa dia membeli kentang dari Maria. (3) Ia dapat setuju untuk merahasiakan pembelian jika Maria mengenakan harga yang lebih rendah. Dalam dua kasus terakhir, Maria dapat memutuskan apakah akan menjual kentang.

Privasi termasuk kontrol informasi tentang diri sendiri. Apakah transaksi itu fakta tentang Maria atau fakta tentang Joe? Tampaknya tidak ada alasan yang meyakinkan bagi salah satu pihak untuk memiliki hak lebih dari yang lain untuk mengontrol informasi tentang transaksi. Namun masalah ini sangat penting untuk keputusan kebijakan hukum tentang penggunaan informasi konsumen. Jika kita menetapkan kontrol atas informasi tentang transaksi kepada salah satu pihak, kita memerlukan landasan filosofis yang kuat untuk memilih pihak mana yang mendapatkannya. (Jika para pihak membuat perjanjian kerahasiaan, maka mereka memiliki kewajiban etis untuk menghormatinya. Jika perjanjian tersebut adalah kontrak hukum, maka mereka memiliki kewajiban hukum untuk menghormatinya.)

Filsuf dan ekonom sering menggunakan transaksi atau hubungan dua orang yang sederhana , seperti skenario Maria / Joe, untuk mencoba memperjelas asas-asas yang terlibat dalam suatu masalah. Apakah pengamatan dan kesimpulan tentang Maria dan Joe menggeneralisasi masyarakat luas dan rumit dan ekonomi global, di mana, sering kali, salah satu pihak dalam transaksi adalah bisnis? Semua transaksi benar-benar di antara orang-orang, meskipun secara tidak langsung. Jadi jika hak properti atau hak privasi dalam informasi tentang transaksi masuk ke salah satu pihak, kita perlu argumen yang menunjukkan bagaimana transaksi dalam ekonomi modern berbeda dengan yang ada di Friendlyville. Kemudian di bagian ini, kami menggambarkan dua sudut pandang pada pengaturan informasi tentang transaksi konsumen: pandangan pasar bebas dan pandangan perlindungan konsumen. Pandangan perlindungan konsumen menyarankan memperlakukan pihak-pihak secara berbeda.

**Kepemilikan data pribadi**

Beberapa ekonom, ahli hukum, dan pendukung privasi mengusulkan memberikan hak properti kepada orang-orang dalam informasi tentang diri mereka. Konsep hak milik dapat berguna bahkan ketika diterapkan pada properti tidak berwujud (kekayaan intelektual, misalnya), tetapi ada masalah dalam menggunakan konsep ini untuk informasi pribadi. Pertama, seperti yang baru saja kita lihat, aktivitas dan transaksi sering melibatkan setidaknya dua orang, yang masing-masing memiliki klaim yang wajar tetapi bertentangan untuk memiliki informasi tentang transaksi. Beberapa informasi pribadi tampaknya bukan tentang transaksi, tetapi masih ada masalah dalam menetapkan kepemilikan. Apakah Anda memiliki ulang tahun Anda? Atau apakah ibumu memilikinya? Setelah semua, dia adalah peserta yang lebih aktif dalam acara tersebut.

Masalah kedua dengan menetapkan kepemilikan informasi pribadi muncul dari gagasan memiliki fakta. (Hak cipta melindungi hak milik intelektual seperti program komputer dan musik, tetapi kita tidak dapat fakta hak cipta.) Kepemilikan fakta akan sangat merusak aliran informasi di masyarakat. Kami menyimpan informasi tentang perangkat elektronik, tetapi kami juga menyimpannya di dalam pikiran kami. Bisakah kita memiliki fakta tentang diri kita sendiri tanpa melanggar kebebasan berpikir dan kebebasan berbicara orang lain?

Meskipun ada kesulitan dalam menetapkan kepemilikan dalam fakta individu, masalah lainnya adalah apakah kita dapat memiliki "profil" kami, yaitu kumpulan data yang menggambarkan aktivitas, pembelian, minat, dan sebagainya. Kita tidak dapat memiliki fakta bahwa mata kita berwarna biru, tetapi kita memiliki hak hukum untuk mengendalikan beberapa kegunaan gambar fotografis kita. Di hampir semua negara bagian, kita memerlukan persetujuan seseorang untuk menggunakan citranya untuk tujuan komersial. Haruskah hukum memperlakukan profil konsumen kita dengan cara yang sama? Haruskah hukum memperlakukan pengumpulan permintaan pencarian kami dengan cara yang sama? Bagaimana kita bisa membedakan antara beberapa fakta tentang pendatang dan “profil”?

Hakim Richard Posner, seorang sarjana hukum yang telah secara ekstensif mempelajari interaksi antara hukum dan ekonomi, memberikan argumen ekonomi tentang bagaimana mengalokasikan hak milik atas informasi.82 Informasi memiliki nilai ekonomi dan pribadi, ia menunjukkan. Penting bagi kita untuk menentukan apakah bisnis, pelanggan, klien, perusahaan, karyawan, dan sebagainya, dapat diandalkan, jujur, dan sebagainya. Interaksi pribadi dan bisnis memiliki banyak peluang untuk keliru dan oleh karena itu mengeksploitasi orang lain. Analisis Posner mengarah pada kesimpulan bahwa, dalam beberapa kasus, individu atau organisasi harus memiliki hak properti atas informasi, sementara dalam kasus lain, mereka tidak seharusnya. Artinya, beberapa informasi harus berada di domain publik. Hak properti dalam informasi adalah tepat ketika informasi memiliki nilai bagi masyarakat dan mahal untuk ditemukan, dibuat, atau dikumpulkan. Tanpa hak kepemilikan atas informasi semacam itu, orang atau bisnis yang melakukan investasi

dalam menemukan atau mengumpulkan informasi tidak akan mendapat keuntungan darinya. Hasilnya adalah orang-orang akan menghasilkan lebih sedikit informasi semacam ini, sehingga merugikan masyarakat. Dengan demikian, undang-undang harus melindungi, misalnya, rahasia dagang, hasil dari banyak pengeluaran dan upaya oleh bisnis. Contoh kedua adalah informasi pribadi, seperti penampilan tubuh telanjang seseorang. Tidak mahal bagi seseorang untuk mendapatkan, tetapi hampir semua dari kita menempatkan nilai untuk melindunginya, dan penyembunyian tidak mahal bagi masyarakat. Jadi masuk akal untuk menetapkan properti tepat di informasi ini kepada individu. Beberapa pendukung privasi ingin melindungi informasi yang dapat menyebabkan penolakan pekerjaan atau semacam layanan atau kontrak (misalnya, pinjaman). Mereka menganjurkan pembatasan berbagi informasi yang dapat memfasilitasi keputusan negatif tentang orang-orang - misalnya, pemilik tanah berbagi database dengan informasi tentang sejarah pembayaran penyewa. Posner berpendapat bahwa seseorang tidak boleh memiliki hak properti untuk informasi pribadi yang negatif atau informasi lain yang penyembunyiannya membantu orang dalam keliru, penipuan, atau manipulasi. Informasi tersebut harus berada dalam domain publik. Itu berarti seseorang seharusnya tidak memiliki hak untuk melarang orang lain mengumpulkannya, menggunakannya, dan meneruskannya, selama mereka tidak melanggar kontrak atau perjanjian kerahasiaan dan tidak memperoleh informasi dengan menguping komunikasi pribadi atau dengan yang lain. sarana terlarang.

Dalam beberapa dekade terakhir, tren dalam undang-undang tidak mengikuti posisi Posner. Beberapa kritikus dari sudut pandang Posner percaya bahwa teori moral, bukan prinsip ekonomi, harus menjadi sumber hak milik.

**Kerangka hukum dasar Kerangka hukum dasar yang**

baik yang mendefinisikan dan menegakkan hak dan tanggung jawab hukum sangat penting bagi masyarakat dan ekonomi yang kompleks dan kuat. Salah satu tugasnya adalah penegakan perjanjian dan kontrak. Kontrak — termasuk kebebasan untuk membentuknya dan penegakan ketentuan mereka oleh sistem hukum — adalah mekanisme untuk menerapkan transaksi ekonomi yang fleksibel dan beragam yang terjadi dari waktu ke waktu dan antara orang-orang yang tidak mengenal satu sama lain dengan baik atau sama sekali.

Kita dapat menerapkan gagasan penegakan kontrak pada kebijakan privasi bisnis dan organisasi yang diterbitkan. Kasus Toysmart adalah contoh. Toysmart, penjual mainan edukasi berbasis Web, mengumpulkan informasi luas tentang sekitar 250.000 pengunjung ke situs webnya, termasuk profil keluarga, preferensi belanja, serta nama dan usia anak-anak. Toysmart telah berjanji untuk tidak merilis informasi pribadi ini. Ketika perusahaan mengajukan kebangkrutan, ia memiliki sejumlah besar utang dan hampir tidak ada aset — kecuali database pelanggannya, yang memiliki nilai tinggi. Para kreditur Toysmart menginginkan basis data dijual untuk mengumpulkan dana guna membayar mereka kembali. Toysmart menawarkan database untuk dijual, menyebabkan badai protes. Konsisten dengan interpretasi bahwa kebijakan Toysmart adalah kontrak dengan orang-orang dalam database, penyelesaian kebangkrutan-pengadilan termasuk penghancuran database.83

Tugas kedua dari sistem hukum adalah menetapkan default untuk situasi yang kontraknya tidak secara eksplisit diliput. Misalkan situs web tidak memposting kebijakan tentang apa yang dilakukannya dengan informasi yang dikumpulkannya. Hak-hak hukum apa yang seharusnya dimiliki oleh operator situs terkait dengan informasi tersebut? Banyak situs dan bisnis offline bertindak seolah-olah defaultnya adalah mereka dapat melakukan apa pun yang mereka pilih. Standar perlindungan privasi adalah bahwa mereka dapat menggunakan informasi hanya untuk tujuan langsung dan jelas yang mereka kumpulkan. Sistem hukum dapat (dan memang) mengatur standar kerahasiaan khusus untuk informasi sensitif, seperti informasi medis dan keuangan, tradisi itu dan kebanyakan orang menganggapnya pribadi. Jika suatu bisnis atau organisasi ingin menggunakan informasi untuk tujuan di luar standar, ia harus menentukan penggunaan tersebut dalam kebijakan, perjanjian, atau kontrak atau meminta persetujuannya. Banyak interaksi bisnis tidak memiliki kontrak tertulis, jadi ketentuan default yang ditetapkan oleh hukum dapat memiliki dampak besar.

Tugas ketiga dari struktur hukum dasar adalah untuk menentukan hukuman atas pelanggaran pidana dan pelanggaran kontrak. Dengan demikian, hukum dapat menentukan hukuman untuk pelanggaran kebijakan privasi dan kelalaian kehilangan atau pengungkapan data pribadi yang disimpan oleh bisnis dan pihak lain. Penulis hukum kewajiban harus mencapai keseimbangan antara terlalu ketat dan terlalu lunak. Jika terlalu ketat, mereka membuat beberapa produk dan layanan berharga terlalu mahal untuk disediakan. Jika terlalu lemah, mereka memberikan insentif yang tidak cukup bagi perusahaan dan lembaga pemerintah untuk memberikan keamanan yang wajar untuk data pribadi kami.

**Peraturan**

Alat teknis, mekanisme pasar, dan kebijakan bisnis untuk perlindungan privasi tidak sempurna. Apakah itu argumen yang kuat untuk hukum peraturan? Regulasi juga tidak sempurna. Kita harus mengevaluasi solusi peraturan dengan mempertimbangkan keefektifan, biaya dan manfaat, dan efek samping, sama seperti kita mengevaluasi jenis lain dari solusi potensial untuk masalah yang disebabkan oleh teknologi. Pro dan kontra peraturan mengisi seluruh buku. Kami secara singkat membuat beberapa poin di sini. (Kita akan melihat masalah serupa di Bagian 8.3.3 ketika kita mempertimbangkan tanggapan terhadap kesalahan dan kegagalan komputer.)

Ada ratusan undang-undang privasi. Ketika Kongres meloloskan undang-undang untuk bidang-bidang kompleks seperti privasi, undang-undang biasanya menyatakan tujuan umum dan menyerahkan rinciannya kepada pemerintah yang menulis ratusan atau ribuan halaman peraturan, kadang-kadang selama bertahun-tahun. Sangat sulit untuk menulis peraturan yang masuk akal untuk situasi yang rumit. Hukum dan

peraturan sering memiliki efek atau interpretasi yang tidak diinginkan. Mereka dapat menerapkan di mana mereka tidak masuk akal atau di mana orang tidak menginginkannya. Peraturan sering memiliki biaya tinggi, baik biaya langsung dolar untuk bisnis (dan, akhirnya, konsumen) dan biaya tersembunyi atau tak terduga, seperti hilangnya layanan atau ketidaknyamanan yang meningkat. Misalnya, peraturan yang melarang perjanjian persetujuan luas dan sebaliknya membutuhkan persetujuan eksplisit untuk setiap penggunaan sekunder informasi pribadi memiliki atribut ekonom menyebut "biaya transaksi tinggi." Persyaratan izin bisa begitu mahal dan sulit untuk diterapkan sehingga menghilangkan sebagian besar penggunaan sekunder dari informasi, termasuk yang diinginkan konsumen.

Meskipun peraturan memiliki kerugian, kita harus ingat bahwa bisnis terkadang melebih-lebihkan biaya peraturan privasi. Mereka juga kadang-kadang meremehkan biaya, untuk diri mereka sendiri dan kepada konsumen, untuk tidak melindungi privasi.

**Sudut Pandang Kontras**

*Ketika ditanya “Jika seseorang menggugat Anda dan kalah, apakah mereka harus membayar*

*biaya hukum Anda?” Lebih dari 80% orang yang disurvei mengatakan “ya.”*

*Ketika ditanya pertanyaan yang sama dari perspektif sebaliknya: “Jika Anda*

*menuntut seseorang dan kalah, apakah Anda harus membayar biaya hukum mereka? ”*

*sekitar 40% mengatakan“ ya. ”*

Pandangan politik, filosofis, dan ekonomi dari banyak cendekiawan dan pendukung yang menulis tentang privasi berbeda. Akibatnya, interpretasi mereka tentang berbagai masalah privasi dan pendekatan mereka terhadap solusi seringkali berbeda, terutama ketika mereka mempertimbangkan hukum dan peraturan untuk mengontrol pengumpulan dan penggunaan informasi pribadi oleh bisnis.*\_* Kami membedakan dua perspektif. Saya menyebutnya pandangan pasar bebas dan pandangan perlindungan konsumen.

**Pandangan pasar bebas**

Orang yang lebih suka solusi berorientasi pasar untuk masalah privasi cenderung menekankan kebebasan individu, sebagai konsumen atau dalam bisnis, untuk membuat kesepakatan sukarela; keragaman selera dan nilai-nilai individu; fleksibilitas solusi teknologi dan pasar; respons pasar terhadap preferensi konsumen; kegunaan dan pentingnya kontrak; dan kekurangan perundangan dan solusi regulasi yang terperinci atau restriktif. Mereka menekankan banyak organisasi sukarela yang menyediakan pendidikan konsumen, mengembangkan pedoman, memantau kegiatan bisnis dan pemerintah, dan tekanan

*\_* Ada cenderung lebih kesepakatan di antara pendukung privasi ketika mempertimbangkan ancaman privasi dan intrusi oleh

pemerintah.

bisnis untuk meningkatkan kebijakan. Mereka mungkin mengambil posisi etis yang kuat tetapi menekankan perbedaan antara peran etika dan peran hukum.

Pandangan pasar bebas untuk pengumpulan dan penggunaan informasi pribadi menekankan persetujuan yang diinformasikan: Organisasi yang mengumpulkan data pribadi (termasuk instansi pemerintah dan bisnis) harus dengan jelas menginformasikan orang yang memberikan informasi jika mereka tidak merahasiakannya (dari bisnis lain, individu, dan lembaga pemerintah ) dan bagaimana mereka akan menggunakannya. Mereka harus bertanggung jawab secara hukum atas pelanggaran kebijakan yang mereka nyatakan. Sudut pandang ini dapat benar-benar mempertimbangkan bentuk-bentuk rahasia pengumpulan informasi tak terlihat menjadi pencurian atau intrusi.

Pandangan pasar bebas menekankan kebebasan kontrak: Orang harus bebas untuk menandatangani perjanjian (atau tidak memasukkan perjanjian) untuk mengungkapkan informasi pribadi dengan imbalan biaya, layanan, atau manfaat lain sesuai penilaian mereka sendiri. Bisnis harus bebas untuk menawarkan perjanjian semacam itu. Sudut pandang ini menghormati hak dan kemampuan konsumen untuk membuat pilihan sendiri berdasarkan nilai-nilai mereka sendiri. Pendukung pasar mengharapkan konsumen untuk mengambil tanggung jawab yang sejalan dengan kebebasan — misalnya, untuk membaca kontrak atau untuk memahami bahwa layanan yang diinginkan memiliki biaya. Pandangan pasar bebas mencakup arus informasi yang bebas: undang-undang tidak boleh mencegah orang (atau bisnis dan organisasi) menggunakan dan mengungkapkan fakta-fakta yang mereka temukan secara independen atau tidak sesuai tanpa melanggar hak (misalnya, tanpa pencurian, pelanggaran, atau pelanggaran kewajiban kontrak).

Kita tidak bisa selalu berharap mendapatkan campuran atribut yang tepat yang kita inginkan dalam produk, layanan, atau pekerjaan apa pun. Sama seperti kita mungkin tidak mendapatkan pizza tanpa rasa takut di setiap restoran pizza atau menemukan mobil dengan fitur yang tepat yang kita inginkan, kita mungkin tidak selalu bisa mendapatkan privasi dan diskon khusus — atau layanan gratis. Kami mungkin tidak dapat memperoleh situs web tertentu — atau majalah — tanpa iklan, atau pekerjaan tertentu tanpa menyetujui untuk memberikan informasi pribadi tertentu kepada perusahaan. Kompromi ini tidak biasa atau tidak masuk akal ketika berinteraksi dengan orang lain.

Pendukung pasar lebih memilih untuk menghindari undang-undang yang membatasi dan peraturan rinci karena beberapa alasan. Peraturan yang terlalu luas, tidak dirancang dengan baik, dan tidak jelas menghambat inovasi. Sistem politik adalah sistem yang lebih buruk daripada pasar untuk menentukan apa yang diinginkan konsumen di dunia nyata dari pertukaran dan biaya. Tidak mungkin bagi legislator untuk mengetahui terlebih dahulu berapa banyak uang, kemudahan, atau manfaat lain yang orang ingin perdagangkan untuk sedikit banyak privasi. Bisnis merespons seiring waktu dengan preferensi jutaan konsumen yang diekspresikan melalui pembelian mereka. Menanggapi keinginan untuk privasi banyak orang menyatakan, pasar menyediakan berbagai alat perlindungan privasi. Pendukung pasar berpendapat bahwa undang-undang yang mensyaratkan kebijakan khusus atau melarang jenis kontrak tertentu melanggar kebebasan memilih baik konsumen dan pemilik bisnis.

Sudut pandang ini termasuk sanksi hukum bagi mereka yang mencuri data dan mereka yang melanggar perjanjian kerahasiaan. Ini memegang bisnis, organisasi, dan agen pemerintah yang bertanggung jawab atas hilangnya data pribadi karena praktik keamanan yang buruk atau lalai. Untuk mendorong inovasi dan peningkatan, para pendukung sudut pandang ini lebih cenderung memilih hukuman ketika perusahaan kehilangan, mengungkapkan secara tidak tepat, atau menyalahgunakan data, daripada peraturan yang menentukan prosedur rinci yang harus diikuti oleh pemegang informasi pribadi.

Sudut pandang pasar bebas melihat privasi sebagai "baik," baik dalam arti bahwa hal itu diinginkan dan bahwa itu adalah sesuatu yang kita dapat memperoleh berbagai jumlah dengan membeli atau perdagangan dalam ekonomi, seperti makanan, hiburan, dan keamanan. Sama seperti beberapa orang memilih untuk memperdagangkan beberapa keamanan untuk kesenangan (bungee jumping, mengendarai sepeda motor), uang (membeli produk yang lebih murah tetapi kurang aman), atau kenyamanan, beberapa memilih tingkat privasi yang berbeda. Seperti halnya keamanan, hukum dapat memberikan standar minimum, tetapi harus memungkinkan pasar untuk menyediakan berbagai pilihan untuk memenuhi berbagai preferensi pribadi.

**Pandangan perlindungan konsumen**

Para pendukung regulasi privasi yang kuat menekankan penggunaan informasi pribadi yang mengganggu yang telah kami sebutkan di sepanjang bab ini, hasil kesalahan yang mahal dan mengganggu dalam basis data (yang kita diskusikan pada Bab 8) dan kemudahan informasi pribadi bocor keluar, melalui kehilangan, pencurian, dan kecerobohan. Mereka berdebat untuk persyaratan izin yang lebih ketat, pembatasan hukum pada profil konsumen, larangan pada jenis kontrak atau perjanjian tertentu untuk mengungkapkan data, dan larangan pada bisnis mengumpulkan atau menyimpan jenis data tertentu. Mereka mendesak, misalnya, bahwa undang-undang mengharuskan perusahaan untuk memiliki kebijakan keikutsertaan untuk penggunaan informasi pribadi sekunder, karena opsi memilih keluar mungkin tidak jelas atau cukup mudah bagi konsumen yang lebih menyukainya. Mereka akan melarang keringanan dan perjanjian persetujuan luas untuk penggunaan sekunder.

Fokus dari sudut pandang ini adalah untuk melindungi konsumen dari pelanggaran dan kecerobohan oleh bisnis dan terhadap kurangnya pengetahuan, penilaian, atau minat mereka sendiri. Para pendukung pandangan perlindungan konsumen menekankan bahwa orang tidak menyadari semua cara orang lain menggunakan informasi tentang mereka. Mereka tidak memahami risiko setuju untuk mengungkapkan data pribadi. Mereka yang menekankan perlindungan konsumen sangat penting terhadap program untuk memperdagangkan perangkat dan layanan gratis untuk informasi pribadi atau persetujuan untuk pemantauan atau pelacakan. Banyak undang-undang dukungan yang melarang pengumpulan atau penyimpanan data pribadi yang dapat memiliki konsekuensi negatif, jika mereka percaya risiko lebih penting daripada nilai informasi untuk bisnis yang ingin mengumpulkannya. Advokat dan privasi konsumen "absolutis" Mary Gardiner Jones keberatan dengan gagasan konsumen menyetujui penyebaran data pribadi. Dia berkata, “Anda tidak dapat mengharapkan konsumen biasa yang sangat sibuk berusaha mencari nafkah untuk duduk dan memahami apa artinya [persetujuan].

Mereka tidak memahami implikasi dari penggunaan data mereka yang berarti bagi mereka. ”85 Dia mengatakan ini kira-kira 20 tahun yang lalu. Memahami implikasi cara data dikumpulkan dan digunakan sekarang lebih sulit. Seorang mantan direktur Proyek Kerahasiaan dan Teknologi ACLU menyatakan pandangan bahwa penjelasan dan persetujuan tidak cukup perlindungan. Dia mendesak komite Senat mempelajari kerahasiaan catatan kesehatan untuk "memeriksa kembali ketergantungan tradisional pada persetujuan individu sebagai inti dari undang-undang privasi."86

Mereka yang menekankan sudut pandang perlindungan konsumen akan berpendapat bahwa skenario Joe / Maria di Friendlyville, dijelaskan sebelumnya di bagian ini, tidak relevan dalam masyarakat yang kompleks. Ketidakseimbangan kekuasaan antara individu dan perusahaan besar adalah salah satu alasannya. Lain adalah bahwa di Friendlyville, informasi tentang transaksi itu hanya bersirkulasi kepada sekelompok kecil orang, yang Joe dan Maria tahu. Jika seseorang menarik kesimpulan yang tidak akurat atau tidak adil, Joe atau Maria dapat berbicara dengan orang tersebut dan menyajikan penjelasannya. Dalam masyarakat yang lebih besar, informasi beredar di antara banyak orang asing, dan kita sering tidak tahu siapa yang memilikinya dan keputusan apa tentang kita yang mendasarkan pada mereka.

Konsumen tidak dapat merundingkan persyaratan kontrak dengan bisnis secara realistis. Pada waktu tertentu, konsumen hanya dapat menerima atau menolak apa yang ditawarkan oleh bisnis. Dan konsumen sering tidak dalam posisi untuk menolaknya. Jika kita menginginkan pinjaman untuk rumah atau mobil, kita harus menerima apa pun yang saat ini ditawarkan oleh pemberi pinjaman. Jika kita membutuhkan pekerjaan, kita cenderung setuju untuk mengungkapkan informasi pribadi terhadap preferensi kita yang sebenarnya karena kebutuhan ekonomi untuk bekerja. Individu tidak memiliki kekuatan yang berarti terhadap perusahaan besar seperti Google dan Apple. Mereka harus menggunakan mesin telusur apakah mereka tahu atau menerima kebijakan perusahaan tentang penggunaan kueri penelusuran mereka.

Dalam pandangan perlindungan konsumen, pengaturan diri oleh bisnis tidak berfungsi. Kebijakan privasi bisnis lemah, tidak jelas, atau sulit dimengerti. Bisnis terkadang tidak mengikuti kebijakan yang mereka nyatakan. Tekanan konsumen terkadang efektif, tetapi beberapa perusahaan mengabaikannya. Sebaliknya, kita harus mewajibkan semua bisnis untuk mengadopsi kebijakan pro-privasi. Perangkat lunak dan alat perlindungan privasi teknologi lainnya untuk konsumen membutuhkan uang, dan banyak orang tidak mampu membelinya. Mereka jauh dari sempurna dan karenanya tidak cukup baik untuk melindungi privasi.

Sudut pandang perlindungan konsumen melihat privasi sebagai hak daripada sesuatu yang kita tawar-menawar. Misalnya, situs web yang disponsori bersama oleh Pusat Informasi Privasi Elektronik dan Privasi Internasional mem-flash slogan “Privasi adalah hak, bukan preferensi” dan “Pemberitahuan tidak cukup.”87 Yang terakhir menunjukkan bahwa mereka melihat privasi sebagai hak positif, atau mengklaim benar (dalam terminologi Bagian 1.4.2). Sebagai hak negatif, privasi memungkinkan kita untuk menggunakan teknologi anonimisasi dan menahan diri untuk tidak berinteraksi dengan mereka yang meminta informasi yang tidak ingin kita berikan. Sebagai hak positif, itu berarti kita dapat menghentikan orang lain untuk berkomunikasi tentang kita. Seorang juru bicara untuk Pusat Demokrasi dan Teknologi menyatakan pandangan itu dalam sebuah pernyataan kepada Kongres, mengatakan bahwa kita harus memasukkan ke dalam hukum prinsip bahwa orang harus dapat "menentukan sendiri kapan, bagaimana dan sejauh mana informasi tentang mereka dibagikan.

### 2.5.3 Peraturan Privasi di Uni Eropa Uni

Eropa (UE) memiliki Arahan Perlindungan Data yang komprehensif (disahkan pada 1995).89 Ini mencakup pemrosesan data pribadi, termasuk pengumpulan, penggunaan, penyimpanan, pengambilan, transmisi, perusakan, dan tindakan lainnya. Arahan menetapkan Prinsip-Prinsip Informasi yang Adil bahwa negara-negara anggota Uni Eropa harus menerapkan dalam hukum mereka sendiri. Beberapa serupa dengan lima prinsip pertama dalam Gambar 2.2 (dalam Bagian 2.1.3). UE memiliki beberapa aturan tambahan atau lebih kuat, termasuk :

* Pemrosesan data diizinkan hanya jika orang tersebut telah menyetujui secara tidak ambigu atau jika pemrosesan diperlukan untuk memenuhi kewajiban kontrak atau hukum atau diperlukan untuk tugas-tugas dalam kepentingan publik atau oleh otoritas resmi untuk menyelesaikan tugas-tugas mereka (atau beberapa alasan lainnya).
* .Kategori data khusus - termasuk asal etnis dan ras, keyakinan politik dan agama, kesehatan dan kehidupan seks, dan keanggotaan serikat - tidak boleh diproses tanpa persetujuan eksplisit orang tersebut. Negara-negara anggota mungkin melarang pemrosesan data tersebut bahkan jika subjek tidak menyetujui.
* . Pengolahan data tentang keyakinan kriminal sangat dibatasi.

Aturan UE lebih ketat daripada di Amerika Serikat, seperti yang diilustrasikan beberapa contoh berikut.

Google memodifikasi kebijakan privasinya pada tahun 2012 untuk memungkinkan perusahaan menggabungkan informasi yang dikumpulkannya pada anggota dari berbagai layanannya. Uni Eropa berpendapat bahwa pengguna rata-rata tidak dapat memahami bagaimana Google menggunakan data mereka di bawah kebijakan baru dan yang melanggar peraturan privasi UE. Pengadilan di Jerman mengatakan bahwa beberapa kebijakan Facebook dalam perjanjian anggotanya (misalnya, pemberian lisensi kepada Facebook untuk menggunakan materi posting anggota atau toko di Facebook) adalah ilegal di sana. Pemerintah Jerman mengatakan kepada Facebook untuk berhenti menjalankan aplikasi pengenalan wajah pada pengguna Jerman; itu melanggar undang-undang privasi Jerman.

Uni Eropa merancang panduan hukum untuk situs jejaring sosial. Pedoman tersebut mengatakan situs harus menetapkan pengaturan privasi default pada tingkat tinggi, memberi tahu pengguna untuk mengunggah gambar seseorang hanya jika orang tersebut mengizinkan, mengizinkan penggunaan psuedonym, menetapkan batas pada waktu mereka menyimpan data pada pengguna yang tidak aktif, dan menghapus akun yang tidak aktif untuk waktu yang lama.

Komisi Eropa mengusulkan pemberian “hak untuk dilupakan” hukum. Ini akan, antara lain, mengharuskan situs web menghapus informasi, foto, dan sebagainya, dari orang tertentu jika orang itu memintanya, apakah orang itu memposting materi atau orang lain melakukannya. Tampaknya juga mengharuskan mesin pencari menghapus tautan ke materi yang ingin dihapus seseorang. "Benar" seperti itu jelas bertentangan dengan kebebasan berbicara dalam kasus-kasus di mana orang lain memposting materi dan tidak ingin itu dihapus.

Sebuah agensi pemerintah Spanyol memerintahkan Google untuk menghapus tautan dari hasil pencarian ke lusinan artikel yang memiliki informasi sensitif tentang orang perorangan. (Google melawan permintaan di pengadilan Eropa, dengan alasan bahwa perintah tersebut melanggar kebebasan berekspresi dan bahwa pemerintah tidak memerlukan media berita untuk menghapus artikel.) Karena undang-undang privasi ketat Jerman, Google Street View memungkinkan siapa saja untuk meminta rumah mereka atau kantor menjadi buram pada gambar jalanannya. Google memenangkan gugatan tentang Street View melanggar privasi pemilik rumah, tetapi perusahaan tersebut menghentikan pengambilan foto untuk Street View di Jerman.

Sementara Uni Eropa memiliki peraturan yang jauh lebih ketat daripada Amerika Serikat tentang pengumpulan dan penggunaan informasi pribadi oleh sektor swasta, beberapa libertarian sipil percaya bahwa peraturan tersebut tidak memberikan perlindungan yang cukup dari penggunaan data pribadi oleh lembaga pemerintah. Meskipun arahan mengatakan bahwa data tidak boleh disimpan lebih lama dari yang diperlukan, negara-negara Eropa mengharuskan ISP dan perusahaan telepon menyimpan catatan komunikasi pelanggan (tanggal, tujuan, durasi, dan sebagainya) hingga dua tahun dan membuatnya tersedia untuk penegakan hukum agensi. Uni Eropa mengatakan perlu persyaratan ini untuk melawan terorisme dan kejahatan terorganisir.

Arahan privasi ketat Uni Eropa tidak mencegah beberapa penyalahgunaan data pribadi yang sama yang terjadi di Amerika Serikat. Di Inggris, misalnya, Komisaris Informasi melaporkan bahwa pialang data menggunakan penipuan dan orang dalam yang korup untuk mendapatkan informasi pribadi. Seperti di Amerika Serikat, pelanggan layanan ilegal termasuk wartawan, penyelidik swasta, penagih utang, lembaga pemerintah, penguntit, dan kriminal yang mencari data untuk digunakan untuk penipuan.92

EU Data Privacy Directive melarang transfer data pribadi ke negara-negara di luar Uni Eropa yang tidak memiliki sistem perlindungan privasi yang memadai. Bagian dari direktif ini menyebabkan masalah signifikan bagi perusahaan yang melakukan bisnis baik di dalam maupun di luar Eropa dan mungkin biasanya memproses data pelanggan dan karyawan di luar UE. Uni Eropa menetapkan bahwa Australia, misalnya, tidak memiliki perlindungan privasi yang memadai. Australia memungkinkan perusahaan untuk membuat kode privasi mereka sendiri yang konsisten dengan Prinsip-Prinsip Privasi Nasional pemerintah. TheUnited States memiliki undang-undang privasi yang mencakup area tertentu seperti informasi medis, penyewaan video, catatan izin mengemudi, dan sebagainya, tetapi tidak memiliki undang-undang privasi komprehensif yang mencakup semua data pribadi. UE menyetujui rencana “Safe Harbor”, di mana perusahaan di luar UE yang setuju untuk mematuhi seperangkat persyaratan privasi yang serupa dengan prinsip-prinsip dalam Petunjuk Perlindungan Data dapat menerima data pribadi dari UE.93 Setelah serangan teroris pada tahun 2001, penyaringan penumpang perjalanan udara dari Eropa ke Amerika Serikat menimbulkan masalah. Pemerintah AS ingin informasi lebih lanjut tentang penumpang daripada Uni Eropa ingin memberikan.

Banyak pendukung privasi menggambarkan kebijakan privasi AS sebagai "di belakang Eropa" karena Amerika Serikat tidak memiliki undang-undang federal yang komprehensif yang mengatur pengumpulan dan penggunaan data pribadi. Yang lain menunjukkan bahwa Amerika Serikat dan Eropa memiliki budaya dan tradisi yang berbeda. Negara-negara Eropa cenderung lebih menekankan pada regulasi dan sentralisasi, terutama mengenai perdagangan, sedangkan tradisi AS lebih menekankan pada kontrak, tekanan konsumen, fleksibilitas dan kebebasan pasar, dan hukuman atas penyalahgunaan informasi pribadi dengan penegakan hukum yang ada (seperti mereka yang menentang praktik bisnis yang menipu dan tidak adil).

## 2.6 Komunikasi

Lembaga penegak hukum memotong komunikasi untuk mengumpulkan bukti kegiatan kriminal. Badan intelijen mencegat komunikasi untuk mengumpulkan informasi tentang kegiatan dan rencana pemerintah yang bermusuhan dan teroris. Amandemen Keempat terhadap Konstitusi AS dan berbagai undang-undang membatasi aktivitas mereka untuk melindungi orang yang tidak bersalah dan mengurangi kesempatan untuk melakukan pelanggaran. Di bagian ini, kami mempertimbangkan bagaimana perubahan teknologi dan kebijakan pemerintah mempengaruhi kemampuan lembaga penegak hukum untuk mencegat konten komunikasi dan untuk memperoleh informasi lain tentang komunikasi. Kami mulai dengan latar belakang tentang penyadapan percakapan telepon dan undang-undang tentang privasi telepon dan e-mail. Kami mempertimbangkan Bantuan Komunikasi untuk Penegakan Hukum Act (CALEA), yang mengharuskan teknologi yang digunakan dalam sistem komunikasi dirancang atau dimodifikasi untuk memastikan kemampuan lembaga penegak hukum untuk mencegat komunikasi. Maka kita menganggap intersepsi komunikasi untuk keamanan nasional.

### 2.6.1 Penyadapan dan Perlindungan Email Telepon

Dalam 10 tahun setelah ditemukannya telepon, orang-orang (keluar masuk pemerintah) sedang menyadap mereka.94 Sebelum itu, orang-orang mencegat komunikasi telegraf. Selama bertahun-tahun ketika para operator manusia membuat sambungan telepon dan kebanyakan orang memiliki saluran partai (satu saluran telepon yang dibagi oleh beberapa rumah tangga), para operator dan tetangga yang suka berang-berang kadang-kadang mendengarkan percakapan telepon.

Meningkatnya kekayaan dan teknologi baru melenyapkan saluran partai dan operator manusia, tetapi telepon masih rentan terhadap penyadapan. Status hukum penyadapan diperdebatkan di sebagian besar abad ke-20. Lembaga penegakan hukum federal dan negara bagian, bisnis, detektif swasta, kandidat politik, dan lainnya banyak digunakan penyadapan. Pada tahun 1928, Mahkamah Agung memutuskan bahwa penyadapan oleh lembaga penegak hukum tidak konstitusional, meskipun Kongres dapat melarangnya. Pada 1934, Kongres mengesahkan UU Komunikasi. Hukum ini menyatakan bahwa, kecuali diizinkan oleh pengirim, tidak ada orang yang dapat mencegat dan membocorkan pesan; tidak ada pengecualian untuk lembaga penegak hukum. Keputusan Mahkamah Agung tahun 1937 memutuskan bahwa penyadapan melanggar hukum ini.95 Agen penegak hukum federal dan negara bagian dan polisi setempat mengabaikan keputusan itu dan terus menyadap secara teratur selama beberapa dekade, kadang-kadang dengan persetujuan dari Jaksa Agung AS. Dalam satu kasus yang dipublikasikan dengan baik, FBI memantau panggilan telepon antara terdakwa dan pengacaranya selama persidangan. Bukti yang diperoleh dengan penyadapan ilegal tidak dapat diadili di pengadilan, sehingga FBI menyimpan sistem file rahasia yang terpisah. FBI menyadap dan menyadap anggota Kongres dan Mahkamah Agung. Meskipun ada publikasi tentang penggunaan luas penyadapan oleh polisi, tidak ada penuntutan yang dihasilkan. Dalam banyak kasus, tentu saja, lembaga penegak hukum sedang menyadap orang-orang yang dicurigai melakukan kejahatan, tetapi dalam banyak kasus lain, mereka menyadap orang-orang dengan pandangan yang tidak biasa, anggota kelompok hak sipil, dan lawan politik pejabat pemerintah yang kuat.

Perdebatan sengit tentang isu penyadapan berlanjut. Kongres berulang kali menolak proposal untuk mengizinkan penyadapan dan pengawasan elektronik. Pada tahun 1967 (dalam *Katz v. Amerika Serikat*, dibahas dalam Bagian 2.2.2), Mahkamah Agung memutuskan bahwa mencegat percakapan telepon tanpa perintah pengadilan melanggar Amandemen Keempat ke Konstitusi AS. Pada tahun 1968, sebagai bagian dari Undang-Undang Kontrol Kejahatan Omnibus dan Safe Streets, Kongres secara eksplisit mengizinkan penyadapan dan pengawasan elektronik oleh lembaga penegak hukum, dengan perintah pengadilan, untuk pertama kalinya dalam sejarah AS. Argumen utama yang diberikan untuk perubahan ini adalah kebutuhan untuk memberantas kejahatan terorganisasi.

Pemerintah membutuhkan perintah pengadilan untuk (secara hukum) memotong atau merekam konten panggilan telepon untuk penyelidikan kriminal.*\_* Agen penegak hukum harus membenarkan permintaan tersebut, dan izin penyadapan diberikan untuk jangka waktu terbatas. Agen pemerintah dapat menentukan nomor telepon yang dipanggil dari telepon tertentu dan nomor dari mana seseorang melakukan panggilan dengan pemeriksaan pengadilan kurang dan pembenaran.

Senator SamErvin berkomentar pada tahun 1968, “Kenyataan bahwa mengesahkan undang-undang tidak pernah menyelesaikan kontroversi yang setajam ini.”96 Dia benar. Perdebatan berlanjut tentang apakah perlindungan privasi dalam UU Kejahatan Omnibus cukup kuat untuk menjadi konstitusional. Hakim agung tidak setuju. Penyadapan oleh pemerintah dan politisi yang ilegal atau legalitas yang dipertanyakan berlanjut, terutama selama Perang Vietnam. Jurnalis dan pegawai pemerintah adalah korban penyadapan inkonstitusional selama pemerintahan Nixon. Pada tahun 1998, petugas polisi Los Angeles mengakui menggunakan penyadapan secara tidak benar dalam sejumlah besar kasus.

Sebagian besar negara lain memiliki perlindungan hukum dan hukum untuk privasi komunikasi, tetapi polisi dan badan intelijen di banyak negara secara rutin melakukan pemantauan ilegal terhadap lawan politik, pekerja hak asasi manusia, dan jurnalis.9

**Email dan komunikasi baru lainnya**

Undang-undang lama tidak secara eksplisit mencakup email dan percakapan telepon seluler, dan penyadapan biasa terjadi ketika email dan telepon seluler baru. Mengemudi di sekitar Silicon Valley yang menguping pembicaraan telepon genggam, dilaporkan, adalah bentuk populer dari kegiatan mata-mata industri pada tahun 1980-an. Snoops menyela percakapan ponsel dari politisi dan selebriti. Undang-Undang Privasi Komunikasi Elektronik tahun 1986 (ECPA), dengan amandemen pada tahun 1994, memperpanjang pembatasan penyadapan tahun 1968 ke komunikasi elektronik, termasuk surat elektronik, telepon tanpa kabel dan telepon seluler, dan perangkat paging. Ini adalah langkah penting untuk melindungi privasi di dunia maya dari pengintaian pribadi dan pemerintah. Itu mengharuskan pemerintah mendapatkan perintah pengadilan untuk email yang dicegat secara hukum.† Kontroversi terus tentang lembaga penegak hukum standar harus bertemu untuk mendapatkan salinan email yang disimpan. Pemerintah berpendapat bahwa orang-orang menyerahkan harapan privasi mereka dengan mengizinkan ISP untuk menyimpan email mereka di komputer ISP; dengan demikian, persyaratan yang ketat dari Amandemen Keempat akan

*\_* Pemerintah dapat mencegat isi komunikasi tanpa perintah pengadilan dalam beberapa keadaan darurat.

† ECPA memungkinkan perusahaan membaca email karyawan di sistem bisnis. Kami membahas masalah

privasi karyawan ini di Bab 6.

tidak berlaku. Pengadilan banding federal memutuskan bahwa orangorang *-memang* memiliki harapan privasi untuk email yang disimpan di ISP mereka dan bahwa polisi membutuhkan surat perintah penggeledahan untuk mendapatkannya.98

Undang-undang PATRIOT AS (yang disahkan segera setelah serangan teroris pada tahun 2001) melemahkan ECPA dan melonggarkan pembatasan pada pengawasan pemerintah dan kegiatan penyadapan. Hal ini memungkinkan agen penegak hukum untuk lebih mudah mendapatkan informasi header (seperti tujuan dan waktu) untuk email. Agen penegak hukum menggunakan standar yang lebih longgar untuk mendapatkan rekaman lokasi ponsel tanpa surat perintah penggeledahan. Praktek ini kontroversial. Beberapa hakim dan pendukung privasi banyak yang berpendapat bahwa ketentuan yang longgar dari ECPA melanggar Perubahan Keempat.

### 2.6.2 Merancang Sistem Komunikasi untuk Interception

Teknologi baru, persaingan pasar, dan beragam kebutuhan pelanggan telah menghasilkan keragaman besar layanan telekomunikasi, peralatan, protokol, algoritma, dan perusahaan. Lembaga penegak hukum berpendapat bahwa teknologi komunikasi yang dikembangkan dalam beberapa dasawarsa terakhir telah membuat tugas mereka dalam mencegat komunikasi dan memperoleh catatan komunikasi (misalnya, nomor telepon yang disebut) lebih sulit. Panggilan telepon internet dan perjalanan email dalam potongan-potongan kecil (disebut paket) bercampur dengan paket-paket dari komunikasi lain. Paket dari satu pesan mungkin mengikuti rute yang berbeda ke tujuan. Jadi, mencegat komunikasi internet lebih sulit daripada memasang klip ke kabel telepon analog lama. Ketika orang menggunakan call forwarding, nomor pertama yang disebut — jumlah agen penegak hukum dapat secara sah mendapatkan cukup mudah (tanpa surat perintah penggeledahan) —tidak memberikan informasi tentang penerima panggilan yang sebenarnya. Bantuan Komunikasi untuk Undang-Undang Penegakan Hukum (CALEA) mensyaratkan bahwa

desain peralatan telekomunikasi memastikan bahwa pemerintah dapat mencegat panggilan telepon (dengan perintah pengadilan atau otorisasi lainnya). CALEA lulus pada tahun 1994, sehingga tidak secara eksplisit mencakup banyak cara berkomunikasi yang lebih baru. Undang-undang itu kontroversial, dan upaya berulang oleh pemerintah untuk memperpanjangnya masih kontroversial. Pada tahun 2010, pemerintah mengusulkan undang-undang untuk mewajibkan situs jejaring sosial dan layanan telepon Internet untuk memodifikasi sistem mereka sehingga agen penegak hukum dapat memantau komunikasi pengguna. Di masa lalu, para insinyur merancang peralatan komunikasi untuk tujuan komunikasinya. FBI mengembangkan alat-alatnya untuk intersepsi, dan penyedia komunikasi harus membantu. Signifikansi CALEA adalah bahwa, sebelumnya, pemerintah tidak dapat mensyaratkan desain dan modifikasi peralatan komunikasi untuk memenuhi intervensi penegakan hukum.

Argumen penting yang mendukung CALEA (dan program pemerintah lainnya untuk mencegat komunikasi) adalah mempertahankan kemampuan lembaga penegak hukum untuk melindungi kita dari pengedar narkoba, kejahatan terorganisir, penjahat lain, dan teroris dalam lingkungan teknologi yang berubah. "Prospek untuk mencoba menegakkan hukum tanpa standar nasional untuk pengawasan akan mengubah penegakan menjadi mimpi buruk," menurut

**The Security of BlackBerrys**

Research inMotion (RIM) menyediakan komunikasi terenkripsi yang sangat aman pada Black-Berrys-nya. Mereka populer di kalangan pebisnis, agen pemerintah, dan pengguna biasa di seluruh dunia. Beberapa pemerintah (termasuk Cina, India, Kuwait, dan Uni Emirat Arab) menekan RIM untuk menyediakan akses ke komunikasi BlackBerry oleh agen pemerintah. Beberapa mengancam akan melarang layanan BlackBerry (dan lainnya) yang tidak dapat mereka pantau. RIM membuat perjanjian dengan beberapa pemerintah untuk memungkinkan akses ke komunikasi pengguna ketika permintaan pemerintah mematuhi undang-undang negara tersebut.

FBI. Masalah dengan CALEA dan program lain untuk mencegat komunikasi, menurut para kritikus, termasuk ancaman terhadap privasi dan kebebasan sipil, potensi penyalahgunaan oleh pemerintah, dan efek samping dari akses "backdoor" yang mengancam keamanan sistem komunikasi. Kritik CALEA juga berpendapat bahwa persyaratan untuk menentukan lokasi fisik pengguna ponsel dan memastikan bahwa pemerintah dapat mencegat komunikasi Internet melampaui ruang lingkup hukum dan memperluas kekuatan pengawasan pemerintah di luar apa yang dimaksudkan Kongres ketika melewati undang-undang. Ide merancang teknologi komunikasi untuk "standar nasional untuk pengawasan" adalah mimpi buruk bagi mereka yang menempatkan nilai tinggi pada privasi dan kebebasan sipil. Haruskah para perancang sistem komunikasi bebas menggunakan teknologi terbaik yang tersedia untuk mencapai kecepatan, kenyamanan, biaya rendah, dan privasi?

Lebih dari 80% dari pengadilan penyadapan yang berwenang untuk investigasi kriminal adalah untuk kasus narkoba.101 Kritikus mengklaim bahwa penyadapan adalah alat penegakan hukum yang kurang bermanfaat daripada informan, pekerjaan detektif, saksi, dan sebagainya. Para pendukung CALEA berpendapat bahwa penyadapan sangat penting untuk menangkap dan / atau menghukum penjahat berbahaya. Fokus penyadapan kriminal pada kejahatan narkoba menimbulkan pertanyaan apakah pemerintah benar-benar membutuhkan kontrol sistem yang begitu luas dan menyeluruh pada sistem komunikasi yang digunakan oleh 300 juta orang Amerika. Jika larangan obat harus diakhiri, seperti larangan alkohol pada tahun 1930-an, apakah kita akan menemukan diri kita sendiri dengan infrastruktur yang mahal dan gangguan keamanan yang mengancam intrusi dan kebutuhan sah yang relatif sedikit untuk itu?

### 2.6.3 Pertemuan NSA dan Agen Rahasia

Tujuan dari National Security Agency (NSA) adalah untuk mengumpulkan dan menganalisis informasi intelijen asing yang terkait dengan keamanan nasional dan untuk melindungi komunikasi pemerintah AS dan informasi sensitif yang terkait dengan keamanan nasional. Karena pemerintah mengenkripsi materi sensitif mereka, NSA telah lama mencurahkan sejumlah besar sumber daya untuk cryptology dan memiliki kemampuan pemecahan kode paling canggih. Sebuah perintah presiden rahasia membentuk NSA pada tahun 1952. Anggarannya masih rahasia, meskipun situs webnya mengatakan NSA / CSS (NSA dan Central Security Service) adalah tentang ukuran salah satu perusahaan Fortune 500 yang lebih besar. NSA membangun dan menggunakan superkomputer yang sangat kuat.*\_* Ini mengumpulkan dan menyimpan banyak sekali informasi.

Beberapa kegiatan NSA melampaui tujuannya — atau menafsirkan tujuan ke tingkat yang sangat luas — dan berpotensi mengancam privasi dan kebebasan warga negara AS. Karena NSA menggunakan metode yang tidak memuaskan Amandemen Keempat, NSA secara hukum dibatasi untuk mencegat komunikasi di luar Amerika Serikat (dengan beberapa pengecualian). Melalui sejarahnya, agensi itu menimbulkan banyak kontroversi dengan secara diam-diam melanggar pembatasan pengawasan orang di Amerika Serikat. Pada 1960-an dan 1970-an, NSA memonitor komunikasi warga Amerika tertentu (termasuk pemimpin hak-hak sipil Martin Luther King Jr. dan penghibur yang menentangVietnam

Perang). Komite Kongres yang diketuai oleh Senator Church menemukan bahwa NSA telah secara diam-diam dan secara ilegal mengumpulkan telegram internasional, termasuk telegram yang dikirim oleh warga Amerika, sejak tahun 1950-an dan mencari informasi intelijen asing dari mereka. Sebagai hasilnya, Kongres meloloskan Foreign Intelligence Surveillance Act of 1978 (FISA) yang menetapkan aturan pengawasan untuk NSA. Undang-undang melarang agensi untuk mengumpulkan massa telegram tanpa surat perintah dan menyusun daftar orang Amerika untuk menonton tanpa perintah pengadilan. Undang-undang menetapkan pengadilan federal rahasia, Pengadilan Pengawasan Intelijen Asing, untuk mengeluarkan surat perintah kepada NSA untuk mencegat komunikasi orang-orang yang dapat ditunjukkannya adalah agen kekuatan asing atau terlibat dalam terorisme atau spionase.

**Akses rahasia ke komunikasi dan catatan komunikasi**

NSA mengumpulkan informasi dengan cara mencegat komunikasi. Sementara beberapa teknologi baru (seperti kabel serat optik) membuat penyadapan lebih sulit, perubahan teknologi lainnya dalam beberapa dekade terakhir membuat komunikasi orang-orang biasa lebih rentan. Komunikasi satelit adalah anugerah bagi NSA; itu bisa mengambil pesan dari udara. Peningkatan kekayaan, perjalanan, dan perdagangan menghasilkan lebih banyak komunikasi internasional — saluran komunikasi yang berantakan dan berpotensi membuat lebih sulit bagi NSA untuk mendeteksi pesan yang menarik. Kemudian, kekuatan pemrosesan komputer yang sangat meningkat memungkinkan NSA untuk memfilter dan menganalisis komunikasi dalam jumlah besar orang yang tidak bersalah, bukan hanya menargetkan tersangka tertentu. Di dunia maya, email kami, percakapan ponsel, tweet, pencarian, pembelian, informasi keuangan, dokumen hukum, dan sebagainya, bercampur dengan komunikasi militer, diplomatik, dan teroris. NSA menyaring semuanya. Itu melakukan "inspeksi paket yang mendalam," menganalisis paket-paket informasi perjalanan melalui Internet, dan mengumpulkan apa pun yang menarik. Ini mengumpulkan semua komunikasi ke dan dari sekitar satu juta orang dalam daftar pengawasannya. Kegiatan intersepsi adalah

*\_* Pada 2012, pemerintah memiliki superkomputer IBM yang beroperasi pada 16,32 petaflops (16,32 juta miliar

operasi per detik), yang secara resmi tercepat di dunia.

sangat kontroversial karena NSA memproses dan mengumpulkan data tentang orang Amerika

tanpa perintah pengadilan dan tidak ada persetujuan dari pengadilan FISA.

Pada tahun 2006, karyawan AT & T mendeskripsikan (di bawah sumpah) sebuah rahasia, ruang aman yang disiapkan NSA di fasilitas switching AT & T. Dari ruangan ini, NSA memiliki akses ke email, telepon, dan komunikasi Web pengguna AT & T.105 NSA membangun basis data telepon dan catatan email jutaan orang Amerika. Pemerintah berpendapat bahwa NSA tidak mencegat atau mendengarkan panggilan telepon dan tidak mengumpulkan informasi identitas pribadi. Ini menggunakan teknologi penambangan data canggih untuk menganalisis pola panggilan untuk belajar bagaimana mendeteksi komunikasi sel teroris. Badan ini menganalisis pola panggilan karena sumber terorisme tersebar dan membutuhkan sarana pendeteksian dan pengawasan yang lebih luas daripada kerja mata-mata lama. NSA tidak dapat lagi bergantung pada pemantauan hanya lalu lintas telepon dari beberapa pemerintah yang bermusuhan dan sejumlah kecil tersangka yang diketahui. Tidak dapat lagi memantau hanya saluran telepon fisik tertentu atau tautan komunikasi yang menghubungkan fasilitas militer tertentu atau tempat menarik lainnya. Analisis lalu lintas komunikasi membantu NSA menentukan apa yang mencurigakan. Para penentang program pemantauan berpendapat bahwa itu adalah gangguan besar pada privasi. Bahkan jika NSA tidak mengumpulkan nama pelanggan, cukup mudah untuk mengidentifikasi kembali orang-orang dari catatan telepon mereka. Para penentang mengatakan pengumpulan catatan tanpa izin oleh NSA

adalah ilegal, dan itu ilegal bagi perusahaan telepon untuk menyediakannya. Beberapa kelompok mengajukan gugatan terhadap AT & T karena melanggar kebijakan privasi dan undang-undang privasi komunikasi yang dinyatakannya dengan membantu NSA.

Kongres meloloskan Undang-Undang Amandemen FISA pada tahun 2008. Undang-undang ini secara retroaktif melindungi AT & T (dan entitas lain yang membantu NSA) dari tuntutan hukum. Meskipun termasuk ketentuan untuk membatasi pengawasan domestik, secara keseluruhan mengurangi perlindungan sebelumnya. Undang-undang Amandemen FISA kontroversial, dan gugatan yang menantang konstitusionalitasnya sedang berlangsung.106 Sementara itu, menjadi jelas bahwa NSA diinstal dan terus mengoperasikan ruang pemantauan rahasia di fasilitas perusahaan telekomunikasi utama AS lainnya, di mana ia dapat menyaring dan mengumpulkan komunikasi domestik apa pun yang dipilihnya.

NSAmembangun pusat data baru yang sangat besar untuk menyimpan, mendekripsi, dan menganalisis miliaran gigabyte komunikasi dan file.107 Apa yang tidak dapat didekripsi sekarang, menyimpannya untuk didekripsi nanti ketika mengembangkan komputer yang lebih cepat atau algoritme yang lebih baik. Para libertarian sipil prihatin bahwa NSA mengumpulkan data bisnis dan pribadi terenkripsi dalam jumlah besar yang tidak ada hubungannya dengan terorisme atau intelijen asing.

Sebelum UU PATRIOT AS, ada batas tajam antara aturan hukum untuk investigasi terorisme (melibatkan orang asing) dan investigasi kriminal (melibatkan orang di Amerika Serikat). UU PATRIOT memungkinkan informasi yang diperoleh dalam investigasi terorisme di bawah perintah FISA untuk digunakan dalam kasus pidana. Pejabat pemerintah tidak mengikuti perlindungan normal dan aturan untuk mencari waran dalam kasus-kasus terorisme. Selain itu, jaksa biasanya memberikan pengacara pembela dalam kasus pidana dengan rekaman pesan yang disadap. Ketika diperoleh sebagai bagian dari kasus terorisme, pemerintah tidak harus memberikan transkrip. Dengan demikian, kekuatan yang lebih luas untuk dilanggar privasi komunikasi dalam investigasi terorisme dapat berdampak serius pada orang dituduh melakukan kejahatan biasa.

Bagaimana kita dapat mengevaluasi program-program NSA dari kumpulan komunikasi yang sangat besar? Bagaimana seharusnya kita bereaksi ketika lembaga pemerintah yang kuat melanggar undang-undang yang melindungi privasi komunikasi? Mengakses data tersangka khusus merupakan bagian yang wajar, penting, dan bertanggung jawab dari investigasi kriminal dan teroris. Akses yang luas dan penggalian data lebih dipertanyakan karena mereka mengancam keamanan dan kebebasan orang yang tidak bersalah jika penyelidik secara keliru memutuskan transaksi seseorang terlihat mencurigakan. Mereka menyediakan mekanisme untuk kontrol totaliter. Apakah kerahasiaan bisa dibenarkan? Apakah kerahasiaan itu penting? Paparan program pemantauan menyebabkan para teroris mengambil langkah-langkah baru untuk menyembunyikan aktivitas, komunikasi, dan transaksi mereka. Kerahasiaan sementara sangat penting untuk banyak investigasi kriminal dan teroris, tetapi program rahasia untuk memantau dan mengumpulkan komunikasi menyajikan potensi besar untuk penyalahgunaan, seperti yang sering kita lihat di masa lalu. Kami juga telah melihat efek mengerikan dari terorisme. Apakah fakta bahwa tidak ada serangan teroris yang berhasil di Amerika Serikat setelah tahun 2001 (sampai saat saya menulis ini) sebagian karena pemantauan komunikasi rahasia dan program analisis NSA dan badan-badan intelijen lainnya?