
3

Kebebasan Berbicara

3.1 Paradigma Komunikasi

3.2 Mengontrol Pidato

3.3 Memposting, Menjual, dan Membocorkan Materi Peka

3.4 Keanoniman

3.5 Net Global: Sensor dan Kebebasan Politik

3.6 Regulasi Netralitas Bersih atau Pasar?

Latihan

3.1 Paradigma Komunikasi

Kongres tidak akan membuat undang-undang. . . meringkas kebebasan berbicara, atau pers.

...

- Amandemen Pertama, Konstitusi AS

Seperti yang kita amati di Bab 1, Internet memberi kita kesempatan luar biasa untuk meningkatkan ekspresi ide secara bebas, komunikasi yang mudah dan murah antara orang-orang dari berbagai negara, dan peluang luar biasa untuk mengakses banyak suara dan sudut pandang di mana-mana. Dunia. Tetapi kebebasan berbicara selalu dibatasi sampai tingkat tertentu di Amerika Serikat dan sebagian besar di banyak negara lain. Dalam bab ini, kami memeriksa bagaimana prinsip kebebasan berbicara dari media sebelumnya mempengaruhi Internet dan bagaimana Internet mempengaruhi mereka. Saya menganggap pornografi di Internet, mencoba untuk membatasi, dan upaya untuk membatasi akses oleh anak-anak; iklan dan perdagangan di Web; spam (massal, email yang tidak diminta); dan anonimitas sebagai perlindungan bagi pembicara. Beberapa bentuk pidato telah lama diperdebatkan (pornografi, misalnya), dan beberapa bentuk baru yang dikembangkan dengan Internet dan teknologi digital lainnya (game spam dan video, misalnya). Ketika Amandemen Pertama melindungi beberapa bentuk pidato kontroversial (seperti video game kekerasan atau membocorkan dokumen sensitif) dari pembatasan hukum, masalah etika dan sosial sangat relevan. Sepanjang bab ini, kami menjelaskan berbagai insiden dan kasus dan mendiskusikan masalah yang mereka angkat. Dalam Bagian 3.5, kami memeriksa bagaimana teknologi komunikasi dan pengawasan mempengaruhi kebebasan berbicara di berbagai negara, terutama beberapa yang memiliki tradisi penyensoran yang panjang.

3.1.1 Mengatur Media Komunikasi

Saat ini hampir klise untuk mengatakan bahwa Internet memungkinkan kita semua menjadi penerbit. Kami tidak perlu mesin cetak mahal atau sistem distribusi yang rumit. Kami hanya membutuhkan komputer atau ponsel. Setiap bisnis, organisasi, atau individu dapat membuat situs web. Kita bisa "mempublikasikan" apapun yang kita inginkan; ini tersedia bagi siapa saja yang memilih untuk membacanya. Pada tahun 1994, sesaat sebelum Web menjadi banyak digunakan, Mike Godwin, yang saat itu seorang pengacara di Electronic Frontier Foundation, menggambarkan perubahan dramatis yang dibawa oleh komunikasi komputer:

Ini adalah media yang jauh berbeda dari telepon, yang hanya satu-ke-satu. -satu sedang, tidak cocok untuk menjangkau banyak orang. Ini adalah media yang jauh berbeda dari surat kabar atau stasiun TV, yang merupakan media satu-ke-banyak, tidak sesuai untuk umpan balik dari para penonton. Untuk pertama kalinya dalam sejarah, kami memiliki banyak-ke-banyak media,

y Meskipun beberapa diskusi kami dalam konteks Amandemen Pertama Konstitusi AS, argumen dan prinsip tentang hak asasi manusia kebebasan berbicara berlaku secara global.

3.1 Komunikasi Paradigma 135

di mana Anda tidak harus kaya untuk memiliki akses, dan di mana Anda tidak harus memenangkan persetujuan dari editor atau penerbit untuk berbicara pikiran Anda. Usenety dan Internet, sebagai bagian dari media baru ini, memegang janji untuk menjamin, untuk pertama kalinya dalam sejarah, bahwa perlindungan Amandemen Pertama terhadap kebebasan pers berarti bagi setiap individu seperti halnya Time Warner, atau untuk Gannett, atau ke New York Times.¹

Individu mengambil keuntungan dari janji itu. Sebagai satu indikasi saja, jumlah blog yang dilewati 150 juta pada tahun 2010.² Beberapa di antaranya dibaca secara luas dan sama berpengaruhnya dengan surat kabar tradisional. Namun, sementara teknologi komunikasi komputer mungkin menjamin kebebasan berbicara dan pers bagi kita semua, jaminannya tidak pasti.

Telepon, film, radio, televisi, kabel, satelit, dan, tentu saja, Internet tidak ada ketika Konstitusi ditulis. Kebebasan pers berlaku bagi penerbit yang mencetak koran dan buku dan “pamflet yang kesepian” yang mencetak dan menyebarkan pamflet yang mengekspresikan ide-ide tidak konvensional. Orang mungkin berpikir Amandemen Pertama harus berlaku untuk setiap teknologi komunikasi baru sesuai dengan semangat dan niatnya: untuk melindungi kebebasan kita untuk mengatakan apa yang kita inginkan. Namun, orang-orang yang kuat secara politik terus berusaha membatasi pembicaraan yang mengancam mereka. Dari Undang-Undang Alien dan Sediasi tahun 1798 hingga pengaturan Komite Aksi Politik, undang-undang tersebut telah digunakan terhadap editor surat kabar yang tidak setuju dengan partai politik yang berkuasa dan melawan kelompok ad hoc dari orang-orang yang berbicara tentang isu-isu. Upaya untuk membatasi kebebasan berbicara dan pers berkembang dengan teknologi baru. Pakar hukum Eric M. Freedman merangkum: “Pengalaman sejarah — dengan mesin cetak, kelompok-kelompok dramatis sekuler, foto, film, musik rock, penyiaran, layanan telepon eksplisit secara seksual, video game, dan media lainnya — menunjukkan bahwa setiap media baru dilihat pada awalnya oleh pemerintah sebagai ancaman yang unik, karena itu secara unik berpengaruh, dan oleh karena itu target sensor yang tepat dan unik.”³

Pada bagian ini, kami memperkenalkan kerangka tiga bagian tradisional untuk perlindungan Amandemen Pertama dan peraturan pemerintah dari media komunikasi yang dikembangkan di Amerika Serikat pada abad ke-20. Seperti yang akan kita lihat, teknologi komunikasi modern dan Internet menuntut agar kerangka kerja diperbarui. Ketiga kategori tersebut adalah:

- Media cetak (surat kabar, buku, majalah, pamflet)
- Siaran (televisi, radio)
- Operator umum (telepon, telegraf, dan sistem pos)

Kategori pertama memiliki perlindungan Amandemen Pertama yang terkuat. Meskipun buku-buku telah dilarang di Amerika Serikat dan orang-orang ditangkap karena mempublikasikan informasi tentang topik-topik tertentu seperti kontrasepsi, kecenderungannya adalah semakin berkurangnya pembatasan pemerintah pada kata tercetak.

y Kumpulan kelompok diskusi Internet awal (pra-Web).

3.1 Paradigma Komunikasi 136

Televisi dan radio mirip dengan surat kabar dalam peran mereka menyediakan berita dan hiburan, tetapi pemerintah mengatur baik struktur industri penyiaran dan isi program. Pemerintah memberikan lisensi penyiaran. Penerima lisensi harus memenuhi standar jasa pemerintah — persyaratan yang tidak akan ditoleransi bagi penerbit karena ancaman nyata terhadap kebebasan berekspresi. Pemerintah telah menggunakan ancaman pencabutan izin untuk mendapatkan stasiun untuk membatalkan talk show berorientasi seksual atau menyensor mereka. Sejak 1971, pemerintah telah melarang iklan rokok dari radio, televisi, dan media elektronik di bawah kendali Federal Communications Commission (FCC), tetapi iklan itu tetap legal di majalah dan surat kabar. Dalam sebuah kasus tahun 1978 yang menantang konstitusionalitas larangan menyiarkan "ketidaksenonohan," Mahkamah Agung menjunjung larangan tersebut. Pemerintah federal sering mengusulkan persyaratan untuk mengurangi kekerasan di televisi atau meningkatkan program untuk anak-anak, tetapi pemerintah tidak dapat menerapkan persyaratan seperti itu. di penerbit cetak. Apakah Anda mendukung atau menentang peraturan tertentu, intinya adalah bahwa pemerintah memiliki kontrol lebih besar atas konten televisi dan radio daripada memiliki lebih dari metode komunikasi yang ada pada saat Bill of Rights ditulis. Argumen utama yang digunakan untuk menolak perlindungan Amandemen Pertama untuk penyiar adalah kelangkaan frekuensi siaran. Hanya ada beberapa saluran televisi dan beberapa frekuensi radio di awal-awal penyiaran. Sebagai ganti hak istimewa "monopoli" menggunakan spektrum langka, yang dimiliki publik, para penyiar diatur dengan ketat. Dengan kabel, satelit, ratusan saluran, dan persaingan dari Internet, argumen yang didasarkan pada kelangkaan dan monopoli tidak relevan sekarang, tetapi preseden kendali pemerintah tetap ada. Argumen kedua, masih digunakan untuk membenarkan pembatasan yang diberlakukan oleh pemerintah terhadap konten, adalah bahwa materi siaran masuk ke dalam rumah dan sulit untuk dijaga dari anak-anak.

Operator umum menyediakan media komunikasi (bukan konten) dan harus menyediakan layanan mereka untuk semua orang. Dalam beberapa kasus, seperti halnya layanan telepon, pemerintah mengharuskan mereka untuk menyediakan "akses universal" (yaitu, untuk mensubsidi layanan bagi orang-orang berpenghasilan rendah). Berdasarkan argumen bahwa operator umum adalah monopoli, hukum melarang mereka mengendalikan konten material yang melewati sistem mereka. Perusahaan telepon dilarang memberikan konten atau layanan informasi dengan alasan bahwa mereka dapat melakukan diskriminasi terhadap penyedia konten pesaing yang juga harus menggunakan saluran telepon mereka. Operator umum tidak memiliki kontrol atas konten, sehingga mereka tidak bertanggung jawab atas konten ilegal yang lewat.

Mulai tahun 1980-an, sistem papan buletin komputer (BBS), layanan komersial seperti CompuServe, Prodigy, dan America Online (AOL), dan akhirnya World Wide Web menjadi arena utama untuk distribusi berita, informasi, dan opini. Karena fleksibilitas besar sistem komunikasi komputer, mereka tidak cocok dengan paradigma penerbitan, penyiaran, dan kereta umum. Televisi kabel menegang kategori ini sebelumnya. Dalam mengomentari undang-undang yang mewajibkan stasiun kabel untuk membawa Anda, FCC telah mendenda komedian George Carlin untuk program radio tentang tujuh kata kotor yang tidak bisa dikatakan di radio.

siaran tertentu, Mahkamah Agung mengatakan operator kabel memiliki lebih banyak kebebasan berbicara daripada penyiar televisi dan radio, tetapi kurang dari penerbit cetak.⁴ Tetapi Web tidak cocok antara kategori yang ada lebih baik daripada yang cocok dalam salah satu dari mereka. Ini memiliki kesamaan dengan ketiganya, serta kemiripan tambahan dengan toko buku, perpustakaan, dan ruang pertemuan yang disewa — semuanya diperlakukan dengan berbeda.

Karena teknologi baru mengaburkan batas-batas teknis antara kabel, telepon, jaringan komputer, dan penyedia konten, hukum mulai beradaptasi. Undang-Undang Telekomunikasi tahun 1996 mengubah struktur peraturan. Ini menghapus banyak divisi hukum buatan dari area layanan dan banyak pembatasan pada layanan yang dapat disediakan oleh perusahaan telekomunikasi. Ini juga secara signifikan mengklarifikasi pertanyaan tentang kewajiban Penyedia Layanan Internet (ISP) dan penyedia layanan online lainnya untuk konten yang diposkan oleh pihak ketiga seperti anggota dan pelanggan. Penerbit dan penyiar cetak secara hukum bertanggung jawab atas konten yang mereka terbitkan atau siarkan. Mereka dapat dituntut karena pencemaran nama baik (membuat pernyataan palsu dan merusak) dan pelanggaran hak cipta, misalnya. Mereka bertanggung jawab secara hukum atas materi tidak senonoh dalam publikasi dan program mereka. Sebelum dikeluarkannya Undang-Undang Telekomunikasi, beberapa orang mengajukan gugatan terhadap operator BBS, ISP, AOL, dan penyedia layanan lainnya untuk konten yang orang lain masukkan ke sistem mereka. Untuk melindungi diri dari tuntutan hukum dan kemungkinan tuduhan kriminal, penyedia layanan mungkin akan keliru karena berhati-hati dan membuang banyak konten yang legal — secara serius membatasi jumlah informasi dan pendapat di dunia maya. Undang-Undang Telekomunikasi menyatakan bahwa "tidak ada penyedia atau pengguna layanan komputer interaktif akan diperlakukan sebagai penerbit atau pembicara dari informasi apa pun yang disediakan oleh penyedia konten informasi lain."⁵ Pernyataan ini menghilangkan ketidakpastian dan penyedia layanan yang dilindungi, sehingga mendorong pertumbuhan konten yang dibuat pengguna.

Pada tahun 1996, bagian utama dari undang-undang penyensoran Internet utama yang pertama, Undang-undang Keputusan Komunikasi, diperintah tidak konstitusional. Namun, upaya untuk menyensor internet terus berlanjut. Kami menyelidiki argumen tentang, serta dampak dari, penyensoran dan undang-undang restriktif lainnya dalam Bagian 3.2. Selain itu, kita akan melihat dalam Bagian 3.2.5 bahwa banyak individu dan pengusaha inovatif yang mencoba untuk mempublikasikan informasi, mengiklankan produk, dan memberikan layanan di Web yang mengalami masalah hukum (dan terkadang denda), bukan karena undang-undang sensor secara eksplisit, tetapi karena undang-undang lama yang membatasi usaha untuk menguntungkan organisasi, bisnis, dan pemerintah yang kuat. Dalam beberapa kasus, konfrontasi antara teknologi baru dan hukum lama menghasilkan peningkatan kebebasan.

3.1.2 Prinsip Pidato Gratis

Saat kami melanjutkan dengan diskusi kami tentang masalah kebebasan berbicara, ada baiknya untuk mengingat beberapa poin penting.

⁴ Penyedia layanan tetap berisiko di banyak negara. Misalnya, kepala eBay di India ditangkap karena seseorang menjual video porno di situs India eBay meskipun video itu sendiri tidak muncul di situs dan penjual melanggar kebijakan perusahaan dengan menjualnya.

3.1 Paradigma Komunikasi 138

Amandemen Pertama ditulis tepat untuk pidato dan gagasan yang menyinggung dan / atau kontroversial. Tidak perlu melindungi pidato dan publikasi yang tidak ada orang yang keberatan. Amandemen Pertama meliputi kata-kata yang diucapkan dan ditulis, gambar, seni, dan bentuk-bentuk ekspresi ide dan pendapat lainnya.

Amandemen Pertama adalah pembatasan kekuasaan pemerintah, bukan individu atau bisnis swasta. Penerbit tidak harus mempublikasikan materi yang mereka anggap menyinggung, ditulis dengan buruk, atau tidak mungkin untuk menarik pelanggan mereka karena alasan apa pun. Penolakan atau pengeditan oleh penerbit tidak melanggar hak Amandemen Pertama penulis. Situs web, perusahaan mesin telusur, dan majalah dapat menolak iklan tertentu jika mereka memilihnya. Itu tidak melanggar kebebasan berbicara pengiklan.

Selama bertahun-tahun dan banyak kasus, Mahkamah Agung telah mengembangkan prinsip dan pedoman tentang ekspresi yang dilindungi. Ketika tindakan atau hukum pemerintah menyebabkan orang-orang menghindari pidato dan publikasi legal karena takut dituntut — mungkin karena undang-undang tidak jelas— tindakan atau hukum dikatakan memiliki "efek mengerikan" pada hak Amandemen Pertama. Pengadilan umumnya memutuskan bahwa undang-undang dengan efek mengerikan yang signifikan tidak konstitusional. Mengadvokasi tindakan ilegal adalah (biasanya) legal; pendengar memiliki kesempatan dan tanggung jawab untuk menimbang argumen dan memutuskan apakah atau tidak untuk melakukan tindakan ilegal. Amandemen Pertama tidak melindungi fitnah dan ancaman langsung, spesifik. Menghasut kekerasan, dalam keadaan tertentu, adalah ilegal. Meskipun Amandemen Pertama tidak membedakan kategori ujaran, pengadilan telah memperlakukan iklan sebagai ucapan "kelas dua" dan pembatasan yang diizinkan yang tidak dapat diterima untuk jenis bahasa lainnya. Namun, kasus-kasus dalam beberapa tahun terakhir telah bertentangan dengan tren itu. Pengadilan telah mulai memutuskan bahwa pembatasan pada iklan yang jujur memang melanggar Amandemen Pertama.⁶ Demikian pula, sejak tahun 1970-an, pemerintah telah mengatur pidato kampanye politik, tetapi keputusan Mahkamah Agung baru-baru ini telah memulihkan beberapa perlindungan Amandemen Pertama untuk itu. Banyak keputusan pengadilan telah melindungi ucapan anonim, tetapi ada upaya serius untuk membatasi atau melarang anonimitas di Internet.

Ada masalah sensor setiap kali pemerintah memiliki atau secara substansial mensubsidi sistem komunikasi atau jaringan (atau layanan kontroversial). Sebagai contoh, pada tahun 1980-an, klinik keluarga berencana bersubsidi federal tidak diizinkan untuk membahas aborsi. Di masa lalu, pemerintah telah membuatnya ilegal untuk mengirim informasi melalui surat yang Amandemen Pertama dinyatakan melindungi. Lembaga federal yang menyediakan dana untuk stasiun radio publik menolak aplikasi universitas karena menyiarkan satu jam seminggu program keagamaan. Dalam Bagian 3.2.2, kita akan melihat bahwa Kongres menggunakan kekuatan pendanaannya untuk mensensor Internet di perpustakaan umum dan sekolah. Terlepas dari sisi masalah yang Anda hadapi, tidak peduli bagaimana perubahan kebijakan dengan presiden atau kongres yang berbeda, intinya adalah bahwa, dalam banyak keadaan, ketika pemerintah membayar, ia dapat memilih untuk membatasi pidato yang seharusnya dilindungi oleh Konstitusi.

⁶ Undang-undang khusus, keputusan pengadilan, dan pedoman adalah rumit dalam beberapa kasus. Diskusi di sini bersifat umum dan disederhanakan.

3.2 Mengontrol Pidato

Saya tidak menyetujui apa yang Anda katakan, tetapi saya akan membela sampai mati hak Anda untuk mengatakannya.

—Guru biografi Voltaire, SG Tallentyre (Evelyn Beatrice Hall), menggambarkan pandangan Voltaire tentang kebebasan berbicara⁷

3.2.1 Pidato Ofensif: Apa itu? Apa itu ilegal?

Apa itu ucapan yang ofensif? Apa yang harus dilarang atau dibatasi oleh hukum di Web? Jawaban tergantung pada siapa Anda. Bisa berupa pidato politik atau agama, pornografi, penghinaan rasial atau seksual, materi Nazi, pernyataan pencemaran nama baik, informasi aborsi, informasi anti-aborsi, iklan minuman beralkohol, iklan secara umum, penggambaran kekerasan, diskusi tentang bunuh diri, atau informasi tentang bagaimana untuk membuat bom. Ada pendukung yang bersemangat untuk melarang masing-masing ini — dan lebih banyak lagi. Negara bagian Georgia berusaha melarang gambar ganja dari Internet. Seorang dokter berargumentasi untuk mengatur diskusi medis di Internet sehingga orang-orang tidak akan mendapatkan saran yang buruk. Pemerintah Cina membatasi pelaporan keadaan darurat (seperti kecelakaan besar atau bencana) dan bagaimana pemerintah menangani mereka. Pemerintah Perancis menyetujui undang-undang yang melarang siapa pun kecuali jurnalis profesional merekam atau mendistribusikan video tindakan kekerasan.

Sebagian besar upaya untuk menyensor Internet di Amerika Serikat, termasuk beberapa undang-undang yang disahkan oleh Kongres, berfokus pada materi pornografi dan materi seksual lainnya, jadi kami menggunakan pornografi sebagai contoh pertama. Banyak dari prinsip yang sama berlaku untuk upaya menyensor jenis material lainnya. Orang-orang membahas aktivitas seksual, dari jenis konvensional dan non-konvensional, termasuk pedofilia, dalam detail grafis di dunia maya. Perbedaan antara kategori seperti erotika, seni, dan pornografi tidak selalu jelas, dan orang yang berbeda memiliki standar pribadi yang sangat berbeda. Ada banyak di Internet yang sangat menyinggung orang dewasa. Beberapa orang ingin melarangnya sama sekali. Beberapa mencari cara untuk menjauhkannya dari anak-anak.

Internet dimulai sebagai forum untuk penelitian dan diskusi ilmiah, sehingga proliferasi pornografi yang cepat mengejutkan beberapa orang. Namun, ini bukanlah perkembangan yang mengejutkan. Bahan yang sama sudah tersedia di majalah dewasa, toko buku, dan bioskop. Sebagai penulis untuk Wired berpendapat, materi seksual dengan cepat menyerang semua teknologi baru dan bentuk-bentuk seni.⁸ Dia menunjukkan bahwa, dari lukisan gua hingga lukisan di Pompeii hingga pahatan batu di Angkor Wat, erotika telah berkembang. Mesin cetak menghasilkan Alkitab dan porno. Fotografi menghasilkan Playboy. Banyak dari kaset video pertama adalah porno. Ratusan ribu situs web berlangganan menyediakan hiburan dewasa.⁹ Apakah semua ini baik atau buruk — apakah itu adalah bagian alami dari sifat manusia atau tanda kemerosotan dan kejahatan, apakah kita harus mentolerir atau mencapnya - adalah moral dan masalah sosial di luar lingkup buku ini. Orang-orang memperdebatkan pornografi tanpa akhir.

tentang isu pornografi dan jenis-jenis ucapan lain yang menyinggung perasaan orang, kami mencoba untuk fokus secara khusus pada masalah-masalah dan masalah-masalah baru yang terkait dengan sistem komputer dan dunia maya.

Apa yang sudah ilegal?

Pada tahun 1973, Mahkamah Agung, di *Miller v. California*, menetapkan pedoman tiga bagian untuk menentukan apakah materi itu tidak senonoh menurut hukum. Amandemen Pertama tidak melindungi materi yang tidak senonoh. Kriteria tersebut adalah (1) menggambarkan tindakan seksual (atau ekskretori) yang penggambarannya secara khusus dilarang oleh hukum negara bagian, (2) menggambarkan tindakan-tindakan ini dengan cara yang menyinggung secara jelas, menarik bagi kepentingan pramuka sebagaimana dinilai oleh orang yang beralasan menggunakan standar komunitas, dan (3) tidak memiliki nilai sastra, seni, sosial, politik, atau ilmiah yang serius. Poin kedua — penerapan standar komunitas — adalah kompromi yang dimaksudkan untuk menghindari masalah menetapkan standar nasional kecabulan di negara yang begitu besar dan beragam. Dengan demikian, kota-kota kecil yang konservatif atau religius dapat membatasi pornografi ke tingkat yang lebih besar daripada daerah perkotaan kosmopolitan.

Sudah lama ilegal untuk membuat, memiliki, atau mendistribusikan pornografi anak. Kami membahas pornografi anak lebih lanjut dalam Bagian 3.2.3, di mana kami mempertimbangkan aplikasi hukum yang tidak diharapkan.

Menegang standar hukum lama

Di Internet, masyarakat tidak memiliki lokasi fisik. Sebaliknya, mereka didefinisikan oleh orang-orang yang memilih untuk berserikat di dunia maya karena kepentingan bersama. Definisi "komunitas" terbukti penting dalam kasus Internet awal. Pasangan di California mengoperasikan sistem papan buletin komputer (BBS) yang disebut Amateur Action yang membuat gambar seksual eksplisit tersedia bagi anggota. Pengamat hukum pada umumnya setuju bahwa operator Amateur Action BBS tidak akan melakukan penuntutan seperti ini berarti bahwa "tidak ada yang dapat dimasukkan ke internet yang lebih tidak masuk akal daripada yang akan ditoleransi dalam komunitas yang paling konservatif di AS" 11 Karena alasan ini, beberapa pengadilan telah mengakui bahwa "standar komunitas" tidak lagi merupakan alat yang tepat untuk menentukan bahan yang dapat diterima. (Untuk standar nasional yang berbeda, lihat Bagian 5.4.1.)

Net juga mengubah arti dari "distribusi". Apakah operator BBS mengirim file cabul

Standar nasional yang berbeda: Bagian 5.4.1

dinyatakan bersalah melakukan kejahatan di California. Inspeksi pos

ke Tennessee? BBS diakses melalui sistem telepon. Siapa saja, dari mana saja, dapat menghubungi

tor di Memphis, Tennessee, bekerja dengan seorang pengacara AS di sana, menjadi anggota BBS (satu-satunya anggota di Tennessee¹⁰) dan mengunduh gambar seksual eksplisit di Memphis. Pasangan itu, yang tinggal dan bekerja di California, diadili di Tennessee dan dinyatakan bersalah mendistribusikan ketaatan di bawah standar komunitas setempat. Keduanya menerima hukuman penjara. Seorang juru bicara untuk Persatuan Kebebasan Sipil Amerika (ACLU) berkomentar bahwa

jika mereka memilih. Inspektur pos di Tennessee memulai panggilan telepon ke BBS dan memulai transfer file. Dia memilih dan mengunduhnya. Kritik terhadap penuntut para opsir BBS berpendapat bahwa seolah-olah inspektur pos pergi ke California, membeli gambar-gambar porno, dan membawa mereka pulang ke Memphis — kemudian penjual itu dituntut di bawah standar komunitas Memphis.¹²

3.2.2 Hukum dan Alternatif Penyensoran

Satu-satunya tujuan kami adalah untuk membuat Internet lebih aman bagi generasi muda kita.

- Jurubicara Departemen Kehakiman¹³

Bahkan di mana perlindungan anak-anak adalah objek, batas konstitusional pada tindakan pemerintah berlaku.

—Justice Antonin Scalia¹⁴ keamanan

Undang-undang sensorutama Pada tahun 1990-an, ketika lebih banyak orang non-teknis mulai menggunakan Internet, berbagai organisasi keagamaan, kelompok antipornografi, dan lainnya memulai kampanye untuk meloloskan undang-undang federal untuk menyensor Internet. Meningkatkan publisitas tentang pornografi di Internet dan meningkatkan tekanan politik menyebabkan Kongres untuk meneruskan Undang-undang Kepadatan Komunikasi (CDA) tahun 1996.¹⁵ Dalam CDA dan undang-undang penyensoran yang diikuti, Kongres berusaha untuk menghindari konflik yang jelas dengan Amandemen Pertama dengan berfokus pada anak-anak. CDA membuat suatu kejahatan untuk membuat tersedia bagi siapa saja yang berusia di bawah 18 setiap komunikasi yang tidak senonoh atau tidak senonoh.

Mungkin sulit untuk merancang undang-undang yang membuat materi yang tidak pantas dari anak-anak sementara memungkinkan akses untuk orang dewasa. Mahkamah Agung memutuskan masalah ini di *Butler v. Michigan*, sebuah kasus 1957 yang mencolok melanggar hukum Michigan yang membuatnya ilegal untuk menjual materi yang mungkin merusak anak-anak. Hakim Frankfurter menulis bahwa negara tidak boleh "mengurangi populasi orang dewasa di Michigan hanya untuk membaca apa yang cocok untuk anak-anak." ¹⁶ CDA membatasi materi tidak senonoh yang dapat diakses oleh anak-anak, tetapi seorang anak dapat mengakses hampir semua hal di Internet. Dengan demikian, lawan mengatakan, itu akan melanggar diktator Justice Frankfurter, tidak hanya di Michigan tetapi di seluruh negeri. Para penentang CDA memberikan contoh-contoh informasi yang legal di media cetak tetapi mungkin menjadi penyebab penuntutan jika tersedia secara online: Alkitab, beberapa drama Shakespeare, dan diskusi serius tentang perilaku seksual dan masalah kesehatan seperti AIDS. Suporter dari CDA berpendapat bahwa ini adalah reaksi berlebihan. Tidak ada yang akan dituntut, kata mereka, untuk materi semacam itu. Kurangnya standar yang jelas, bagaimanapun, dapat menyebabkan penuntutan yang tidak adil dan tidak adil. Ketidakpastian tentang potensi penuntutan bisa memiliki efek dingin pada mereka yang memberikan informasi untuk orang dewasa yang mungkin tidak cocok untuk anak-anak.

Mahkamah Agung memutuskan dengan suara bulat, dalam *American Civil Liberties Union et al. v. Janet Reno*, bahwa ketentuan penyensoran CDA tidak konstitusional. Pengadilan membuat pernyataan kuat tentang pentingnya melindungi kebebasan berekspresi secara umum dan di Internet. Keputusan terhadap CDA menetapkan bahwa "Internet layak mendapat perlindungan tertinggi dari campur tangan pemerintah."

- . Bedakan ucapan dari tindakan. Advokasi tindakan ilegal adalah (biasanya) legal.
- . Hukum tidak boleh mendinginkan ekspresi pidato hukum.
- . Jangan mengurangi orang dewasa hanya untuk membaca apa yang cocok untuk anak-anak.
- . Memecahkan masalah bicara dengan cara yang paling tidak membatasi.

Gambar 3.1 Panduan kebebasan berbicara.

Gambar 3.1 merangkum prinsip-prinsip yang digunakan pengadilan untuk membantu menentukan apakah undang-undang sensor bersifat konstitusional. Ketika pemerintah mengejar tujuan yang sah yang mungkin melanggar kebebasan berbicara (dalam hal ini, perlindungan anak-anak), pemerintah harus menggunakan cara yang paling tidak terbatas untuk mencapai tujuan. Pengadilan menemukan bahwa perangkat lunak penyaringan yang baru dikembangkan kurang ketat dan lebih diinginkan daripada penyensoran. Para hakim juga berkomentar, "Pemerintah dapat terus melindungi anak-anak dari pornografi di Internet melalui penegakan hukum yang kuat yang mengkriminalisasi kecabulan dan pornografi anak."

17

Kongres mencoba lagi, dengan Undang-undang Perlindungan Anak Online (COPA), pada tahun 1998. Ini hukum lebih terbatas daripada CDA. COPA menjadikannya kejahatan federal untuk situs web komersial agar tersedia bagi anak di bawah umur yang "berbahaya bagi anak di bawah umur" sebagaimana dinilai oleh standar komunitas. Sekali lagi, pendukung Amandemen Pertama berpendapat bahwa undang-undang itu terlalu luas dan akan mengancam seni, berita, dan situs kesehatan. Pengadilan yang mengevaluasi COPA mencatat bahwa karena Web dapat diakses di mana-mana, ketentuan standar komunitas akan membatasi seluruh negara ke standar komunitas yang paling konservatif. Pengadilan mengatakan COPA membatasi akses ke sejumlah besar pidato online yang sah menurut hukum untuk orang dewasa, dan persyaratan COPA bahwa orang dewasa memberikan identifikasi untuk melihat materi yang tidak sesuai untuk anak di bawah umur akan memiliki efek tidak konstitusional yang mencemarkan kebebasan berbicara. Setelah lebih dari 10 tahun tuntutan hukum dan banding, Mahkamah Agung menolak untuk mendengar banding terakhir pemerintah, dan COPA meninggal pada tahun 2009.

Kongres mengeluarkan Undang-Undang Perlindungan Internet Anak-Anak (CIPA) pada tahun 2000 untuk meminta perpustakaan dan sekolah menggunakan perangkat lunak filter di Internet terminal. Ketika perpustakaan umum pertama kali memasang terminal Internet, ada masalah. Orang menggunakan terminal untuk melihat gambar "X-rated", dalam pandangan anak-anak atau pengguna perpustakaan lain yang menganggapnya ofensif. Beberapa orang mengikat terminal selama berjam-jam untuk melihat materi tersebut sementara yang lain menunggu untuk menggunakan terminal. Anak-anak mengakses materi seksual dewasa. Anak-anak dan orang dewasa mengakses situs politik ekstremis dan materi rasis. Pustakawan di seluruh negeri berusaha memuaskannya pengguna perpustakaan, orang tua, organisasi masyarakat, libertarian sipil, dan Perpustakaan Hak Cipta mereka sendiri (yang menentang membatasi akses ke bahan pustaka karena usia). Beberapa memasang filter polarisasi pada terminal atau dinding yang dibangun di sekitar terminal sehingga layar hanya dapat dilihat dari depan secara langsung (keduanya untuk melindungi privasi

pengguna dan untuk melindungi pengguna dan karyawan lain dari materi yang mereka anggap tidak pantas). Sebagian besar menetapkan batasan waktu pada penggunaan terminal. Beberapa pustakawan meminta pelanggan untuk berhenti menonton pornografi, seperti ketika mereka meminta seseorang untuk berhenti membuat keributan. Beberapa perangkat lunak pemfilteran yang terpasang di semua terminal, beberapa hanya pada terminal di bagian anak-anak. Beberapa pengawasan orang tua yang diharuskan untuk anak-anak menggunakan Internet, dan beberapa izin orang tua yang diminta.

CIPA berusaha mengganti metode-metode ini. Para penulis CIPA berusaha untuk menghindari keberatan pengadilan terhadap CDA dan COPA dengan menggunakan kekuatan pendanaan pemerintah federal. CIPA mengharuskan sekolah dan perpustakaan yang berpartisipasi dalam program federal tertentu (menerima uang federal untuk teknologi) memasang perangkat lunak penyaringan di semua terminal internet untuk memblokir akses ke situs dengan pornografi anak, materi cabul, dan materi "berbahaya bagi anak di bawah umur." Tentu saja, banyak sekolah dan perpustakaan bergantung pada dana tersebut. Organisasi kebebasan sipil dan American Library Association menggugat untuk memblokir CIPA.¹⁸ Mahkamah Agung memutuskan bahwa CIPA tidak melanggar Amandemen Pertama. CIPA tidak memerlukan penggunaan filter. Itu tidak memaksakan penjara atau denda pada orang-orang yang menyediakan konten di Internet. Ini menetapkan syarat untuk menerima dana federal tertentu. Pengadilan sering menerima kondisi seperti itu. Pengadilan menyatakan dengan jelas bahwa jika seorang dewasa meminta pustakawan untuk menonaktifkan filter di perpustakaan Internet terminal yang digunakan orang dewasa, pustakawan harus melakukannya. Tentu saja, beberapa orang dewasa tidak menyadari adanya perangkat lunak filter, tidak sadar bahwa mereka dapat secara legal memintanya untuk dimatikan, atau tidak mau menarik perhatian mereka sendiri dengan membuat permintaan.

Di luar sekolah umum dan perpustakaan, kecenderungan keputusan pengadilan adalah memberikan perlindungan Amandemen Pertama di Internet yang mirip dengan media cetak, yaitu tingkat perlindungan tertinggi.

Video game

Video game yang kasar telah menjadi fokus kritik sejak mereka mulai muncul. Beberapa sangat berdarah; beberapa menggambarkan pembunuhan dan penyiksaan; beberapa fokus pada kekerasan terhadap perempuan dan anggota kelompok etnis dan agama tertentu. Apakah mereka buruk untuk anak-anak? Apakah mereka lebih berbahaya daripada bentuk-bentuk kekerasan lain dan seksisme dan rasisme keras yang dipelajari anak-anak di buku-buku atau media lain? Haruskah kita melarang mereka?

Beberapa berpendapat bahwa interaktivitas permainan video memiliki dampak yang lebih kuat pada anak-anak daripada menonton televisi secara pasif atau membaca cerita kekerasan. Yang lain menunjukkan bahwa anak-anak telah bermain saling membunuh (polisi dan perampok, koboi dan India) selama beberapa generasi. Apakah terjatuh "mati" di rumput dibandingkan dengan permainan video game yang berulang-ulang dan eksplosif? Pada usia berapa seorang anak cukup dewasa untuk memutuskan untuk memainkan permainan video kekerasan: 12? 18? Siapa yang harus memutuskan permainan apa yang dimainkan anak-anak: orang tua atau legislator? Orangtua tidak selalu bersama anak-anak mereka. Mereka secara teratur khawatir bahwa tekanan teman sebaya mengesampingkan aturan dan bimbingan orang tua.

Undang-undang California melarang penjualan atau penyewaan video game kekerasan kepada anak di bawah umur. Pada tahun 2011, Mahkamah Agung memutuskan bahwa hukum melanggar Amandemen Pertama. Pengadilan menunjukkan

bahwa kekerasan dan gore adalah hal yang umum dalam dongeng klasik (misalnya, Grimm Brothers yang muram), kartun (Elmer Fudd selalu menembaki Bugs Bunny), komik superhero, dan remaja sastra wajib membaca di SMA. Banyak video game yang sangat menjijikkan, tetapi Pengadilan mengatakan bahwa "jijik bukanlah dasar yang valid untuk membatasi ekspresi." 19 Pengadilan mempertimbangkan penelitian tentang dampak gim video pada perasaan agresif anak-anak dan menemukan bahwa dampaknya kecil dan sedikit berbeda dari dampak media lain.

Alternatif untuk penyensoran

Apa alternatif untuk penyensoran yang tersedia untuk melindungi anak-anak dari materi yang tidak pantas di Internet (dan untuk melindungi orang dewasa dari materi yang menyinggung mereka)?

Apakah Berbicara tentang bom - atau pertanian

Beberapa teroris yang memasang bom di Amerika Serikat dan negara lain meneliti teknik pembuatan bom di Internet. Siswa yang membawa bom ke sekolah-sekolah belajar cara membuatnya di Internet. Sejauh tahun 1995, dalam beberapa minggu setelah pemboman gedung federal Kota Oklahoma, terorisme dan subkomite teknologi Senat mengadakan dengar pendapat tentang "Ketersediaan Pembuatan Bom Informasi di Internet." Ada banyak kesamaan antara kontroversi tersebut. tentang informasi pembuatan bom di Internet dan kontroversi tentang pornografi. Seperti pornografi, informasi pembuatan bom sudah tersedia luas di media tradisional, dilindungi oleh Amandemen Pertama. Ini juga memiliki kegunaan yang sah. Informasi tentang cara membuat bom dapat ditemukan dalam versi cetak Encyclopedia Britannica dan dalam buku-buku di perpustakaan dan toko buku. Departemen Pertanian AS mendistribusikan sebuah buku kecil yang disebut "Buku Pegangan Blasters" — para petani menggunakan peledak untuk menghilangkan tunggul pohon.²⁰

Berdebat untuk menyensor informasi tentang bom di Internet, Senator Dianne Feinstein berkata, "Ada perbedaan antara kebebasan berbicara dan mengajar seseorang untuk membunuh."²¹ Berdebat melawan sensor, seorang mantan pengacara AS mengatakan bahwa "informasi-plus," (yaitu informasi yang digunakan dalam komisi tindakan kriminal) adalah apa yang harus diatur oleh hukum. Senator Patrick Leahy menekankan bahwa itu adalah "perilaku berbahaya dan berbahaya, bukan ucapan, yang membebani konsekuensi hukum yang merugikan." Ini sudah, pada dasarnya, prinsip hukum yang didirikan di luar dunia maya. Tentu saja ada undang-undang yang melarang penggunaan bom untuk membunuh orang atau menghancurkan properti, serta undang-undang yang melarang membuat bom atau bersekongkol untuk membuatnya untuk tujuan tersebut.

Kongres mengesahkan undang-undang yang mewajibkan 20 tahun penjara bagi siapa saja yang mendistribusikan informasi pemboman mengetahui atau berniat bahwa itu akan digunakan untuk melakukan kejahatan. Meskipun telah ada beberapa insiden sejak saat itu di mana orang-orang membangun dan menggunakan bom yang dibuat dengan informasi dari Internet, tidak ada yang diadili di bawah undang-undang ini.²² Sulit untuk menentukan (dan membuktikan) apa yang orang posting informasi yang tahu dan berniat tentang penggunaannya.

ada solusi yang tidak mengancam untuk mengurangi diskusi bebas dari subyek serius atau menolak materi seksual eksplisit untuk orang dewasa yang menginginkannya? Seperti yang kita lihat untuk banyak masalah, ada berbagai solusi berdasarkan pasar, teknologi, tanggung jawab, dan pendidikan, serta penegakan hukum yang ada.

Pengembangan filter perangkat lunak adalah contoh respons pasar yang cepat terhadap suatu masalah. Banyak keluarga dengan anak-anak menggunakan perangkat lunak penyaringan (beberapa di antaranya gratis). Filter perangkat lunak bekerja dalam berbagai cara. Mereka dapat memblokir situs web dengan kata-kata, frasa, atau gambar tertentu. Mereka dapat memblokir situs menurut berbagai sistem rating. Mereka dapat berisi daftar panjang situs tertentu untuk diblokir. Orangtua dapat memilih kategori untuk difilter (misalnya, jenis kelamin atau kekerasan), menambahkan daftar mereka sendiri dari situs yang terlarang, dan meninjau log aktivitas anak mereka. Tetapi filter tidak dapat melakukan pekerjaan yang sempurna. Faktanya, pada awalnya, banyak yang melakukan pekerjaan yang sangat buruk. Mereka terlalu banyak menyaring (situs tentang Middlesex dan Essex) dan terlalu sedikit (kehilangan beberapa materi yang jelas tidak menyenangkan). Filter situs yang diblokir berisi diskusi politik dan materi pendidikan (misalnya, halaman beranda dari departemen biologi universitas dan situs web kandidat untuk Kongres yang berisi pernyataan tentang aborsi dan kontrol senjata). Filter membaik seiring waktu, tetapi tidak mungkin untuk sepenuhnya menghilangkan kesalahan dan pandangan subjektif tentang apa yang terlalu seksual atau terlalu keras atau terlalu kritis terhadap agama, informasi medis apa yang cocok untuk anak-anak pada usia berapa, apa yang dapat dikatakan tentang homoseksualitas, dan seterusnya. Tidak ada solusi yang kami jelaskan dalam buku ini untuk masalah yang dihasilkan oleh teknologi baru yang sempurna. Mereka memiliki kekuatan dan kelemahan dan berguna dalam beberapa keadaan dan bukan yang lain. Orang tua dapat menimbang pro dan kontra dan membuat pilihan mereka. Namun kelemahannya - terutama pemblokiran materi hukum - memang menghadirkan masalah kebebasan berbicara ketika para legislator memandatkan filter atau ketika lembaga publik menggunakan filter.

Operator nirkabel menetapkan standar "kesusilaan" ketat bagi perusahaan yang menyediakan konten untuk jaringan mereka. Aturan mereka rinci dan ketat dari apa yang dapat dilarang oleh pemerintah.²³ Layanan komersial, komunitas online, dan situs jejaring sosial mengembangkan kebijakan untuk melindungi anggotanya. Metode termasuk mengeluarkan pelanggan yang memposting atau mengirim materi yang dilarang oleh undang-undang atau kebijakan situs, menghapus materi ofensif, dan membantu penegakan hukum dengan investigasi pornografi anak atau upaya untuk bertemu dan menganiaya anak-anak. Situs jejaring sosial mengembangkan teknologi untuk melacak anggota yang memposting pornografi anak. Sebagai tanggapan terhadap permintaan pasar, perusahaan menawarkan layanan online, situs web, dan layanan telepon seluler yang ditargetkan untuk keluarga dan anak-anak. Beberapa memungkinkan pelanggan untuk mengunci anak-anak keluar dari area tertentu. Orangtua dapat mengatur akun tanpa email untuk anak-anak mereka atau membuat daftar alamat yang ditentukan dari mana akun anak-anak mereka dapat menerima email. Industri video game mengembangkan sistem rating yang memberikan indikasi bagi orang tua tentang jumlah seks, tidak senonoh, dan kekerasan dalam sebuah gim.²⁴ Beberapa situs gim daring membatasi tawaran mereka untuk permainan non-kekerasan dan mengiklankan kebijakan itu. Banyak layanan online mendistribusikan informasi dengan tips tentang cara mengontrol apa yang dilihat anak-anak. Situs-situs dari

3.2 Pidato Pengawasan 3.2

FBI dan organisasi seperti National Center for Missing and Exploited Children²⁵ memberikan informasi tentang risiko kepada anak-anak dan panduan untuk mengurangnya.

Orangtua memiliki tanggung jawab untuk mengawasi anak-anak mereka dan mengajari mereka cara menangani materi dan ancaman yang tidak pantas. Tetapi teknologi tentu telah mengubah risiko pada anak-anak dan membuat pekerjaan orang tua lebih sulit. Jika seorang anak kecil mencoba membeli tiket untuk film X-rated di bioskop atau membeli majalah dewasa di toko, kasir akan melihat anak itu dan menolak (setidaknya, sebagian besar waktu). Di supermarket atau taman bermain, orang tua atau pengamat lain mungkin melihat seorang "orang asing" berbicara dengan seorang anak. Seorang penganiaya anak yang berpotensi online tidak terlihat. Rumah itu dulunya adalah tempat berlindung yang aman dari pornografi dan materi kekerasan atau kebencian. Orangtua dapat bersantai ketika seorang anak bermain di kamar tidurnya. Dengan koneksi Internet dan ponsel, itu tidak lagi benar.

3.2.3 Pornografi Anak dan Sexting

Pornografi anak mencakup gambar atau video anak di bawah umur yang sebenarnya (anak-anak di bawah 18 tahun) yang terlibat dalam perilaku seksual eksplisit. Hukum untuk menciptakan, memiliki, atau mendistribusikan pornografi anak mendahului Internet. Mereka mencakup berbagai macam gambar, banyak yang tidak akan memenuhi definisi materi tidak senonoh secara ilegal jika orang yang digambarkan adalah orang dewasa.

Produksi pornografi anak adalah ilegal terutama karena produksinya dianggap pelecehan anak-anak yang sebenarnya, bukan karena dampak dari konten pada pemirsa. Orang dewasa yang memproduksi pornografi anak sering memaksa atau memanipulasi anak-anak untuk berpose atau tampil. (Kepemilikan pornografi anak tidak secara langsung menyalahgunakan anak-anak, tetapi Mahkamah Agung menerima larangan kepemilikan atas argumen bahwa pembeli atau pengguna gambar mendorong produksi mereka.) Tidak secara otomatis ilegal untuk membuat atau mendistribusikan film seksual eksplisit atau foto di mana aktor dewasa memainkan minor. Dengan kata lain, dasar hukum untuk undang-undang pornografi anak adalah untuk mencegah menggunakan, menyalahgunakan, dan mengeksploitasi anak-anak, tidak menggambarkannya. Agen penegak hukum secara teratur melakukan penangkapan untuk distribusi pornografi anak melalui email, ruang obrolan, media sosial, dan ponsel. Mereka menggunakan pengawasan, surat perintah penggeledahan, operasi penyerangan, dan penyamaran investigasi untuk membangun kasus mereka dan melakukan penangkapan. Kongres memperluas undang-undang melawan pornografi anak untuk memasukkan anak-anak "virtual", yaitu gambar-gambar yang dihasilkan komputer yang tampak seperti anak di bawah umur, serta gambar-gambar lain di mana orang dewasa sebenarnya tampak di bawah umur. Mahkamah Agung memutuskan bahwa ini melanggar Amandemen Pertama. Justice Anthony Kennedy berkomentar bahwa penyuluhan ini "melarang penggambaran visual dari sebuah ide — bahwa remaja terlibat dalam aktivitas seksual — itu adalah fakta masyarakat modern dan telah menjadi tema dalam seni dan sastra sepanjang zaman." ²⁶

Ini adalah penyederhanaan. Undang-undang mencakup lebih detail dan definisi.

Namun, Pengadilan menerima undang-undang kemudian yang memberikan hukuman keras untuk kategori tertentu gambar yang dihasilkan komputer dan gambar kartun yang tampak di bawah umur.

Sexting berarti mengirim teks atau foto yang secara seksual sugestif atau eksplisit, biasanya melalui telepon seluler atau media sosial. Fenomena yang kita diskusikan di sini melibatkan anak-anak, terutama remaja di bawah 18 tahun, mengirim foto-foto telanjang atau semi-formal tentang diri mereka sendiri atau pacar atau pacar mereka satu sama lain atau kepada teman sekelas. Praktik ini mengerikan bagi orang tua, yang mengenali bahaya yang ditimbulkannya pada anak-anak mereka. Salah satu hasil umum dari sexting adalah memalukan dan mengejek ketika gambar-gambar itu didistribusikan secara luas. Dalam kasus ekstrim, setelah mantan pacar membagikan foto seorang gadis 18 tahun, dia bunuh diri. Banyak anak muda (seperti banyak orang dewasa) tidak memikirkan tentang betapa cepatnya sesuatu yang ditumbuhkan untuk satu orang atau sekelompok kecil menyebar ke khalayak yang besar, tidak juga betapa sulitnya untuk menghapus sesuatu dari dunia maya begitu berada di luar sana. Mereka tidak memikirkan dampak untuk hubungan pribadi dan karir masa depan mereka.

Undang-undang pornografi anak dimaksudkan untuk diterapkan pada orang dewasa yang melakukan pelanggaran terhadap anak-anak. Tetapi ponsel dan sexting menyebabkan penerapan hukum dengan cara yang tidak diantisipasi. Jaksa telah membawa tuduhan pornografi anak terhadap anak-anak karena sexting. Kepemilikan pornografi anak adalah ilegal, sehingga anak-anak yang memiliki foto teman di bawah 18 tahun di telepon mereka yang menurut jaksa memenuhi definisi pornografi anak berpotensi melanggar. Apakah mengirimkan foto-foto nude atau foto-foto seksual sugestif suatu bentuk ekspresi? Apakah itu perilaku yang bodoh dan berpotensi merusak oleh orang yang belum dewasa yang harus ditangani oleh orang tua dan pejabat sekolah? Haruskah itu menjadi kejahatan kriminal dengan hukuman berat yang dapat termasuk dimasukkan ke dalam database pelanggar seks selama bertahun-tahun?

Beberapa jaksa mungkin melihat ancaman penuntutan sebagai satu-satunya alat yang mereka miliki untuk menghentikan orang-orang muda melakukan sesuatu yang sangat mereka sesali di masa depan. Beberapa mungkin memaksakan standar moral mereka pada anak-anak orang lain. Dalam satu kasus, seorang gadis 14 tahun dituntut setelah menolak kesepakatan yang mengharuskan dia menghadiri kelas konseling dan menulis esai tentang tindakannya. Pengadilan memutuskan bahwa menggunakan ancaman penuntutan dengan cara ini adalah untuk memaksa pidato (esai) dan, dengan demikian, melanggar Amandemen Pertama. Alat-alat yang mungkin berguna di sekolah-sekolah yang berusaha mencegah sexting (seperti konseling dan esai) tidak dapat diterima ketika dipaksakan oleh pemerintah. Badan legislatif di beberapa negara bagian telah merevisi undang-undang negara mereka dengan berbagai cara untuk mengurangi hukuman karena sexting. Detail bervariasi. Misalnya, ada yang menjadikannya sebagai pelanggaran ringan, bukan kejahatan, jika orang muda mengirim foto ilegal ke orang muda lain dengan usia yang sama. Beberapa telah mengurangi atau menghilangkan hukuman jika foto didistribusikan (di antara anak di bawah umur) dengan persetujuan dari orang dalam gambar. Merevisi undang-undang pornografi anak untuk menangani seks dengan tepat adalah penting, tetapi itu saja tidak cukup. Sexting, dan terutama mendistribusikan foto-foto eksplisit dari teman sekolah dengan maksud untuk memermalukan mereka,

y Sexting tentu tidak terbatas pada remaja. Setidaknya dua anggota Kongres telah mengundurkan diri karena skandal seks.

adalah masalah yang harus diatasi melalui pendidikan tentang konsekuensi dari tindakan seperti itu, keterlibatan orang tua, kebijakan sekolah, hukuman yang masuk akal, dan sebagainya.

3.2.4 Spam

Apa masalahnya?

Istilah spam, dalam konteks komunikasi elektronik, diadopsi pada 1990-an menjadi email massal yang tidak diminta. Sekarang, ini berlaku untuk pesan teks, tweet, dan panggilan telepon juga. Detail dari definisi yang tepat, tergantung pada bagaimana seseorang mendefinisikan "bulk" dan "unsolicited," dapat menjadi penting untuk diskusi tentang bagaimana menangani spam, terutama ketika kita mempertimbangkan hukum untuk membatasinya.

Spam telah membuat marah pengguna Internet sejak tahun 1990-an. Sebagian besar, tetapi tidak semua, spam adalah iklan komersial. Spam dikembangkan karena email sangat murah dibandingkan dengan iklan direct mail yang dicetak. Beberapa bisnis dan organisasi mengumpulkan atau membeli daftar alamat email yang sangat besar dan mengirim pesan yang tidak diminta. Beberapa daftar pembuatan dengan menggunakan perangkat lunak otomatis yang menjelajahi Web dan mengumpulkan apa pun yang terlihat seperti alamat email.

Spam membuat orang marah karena konten dan cara pengirimannya. Konten dapat berupa iklan komersial biasa, iklan politik, permohonan dana dari organisasi nonprofit, pornografi, dan iklan untuknya, penipuan "dapatkan cepat kaya" penipuan, dan penipuan yang menjual produk palsu atau tidak ada. Topik datang dalam gelombang, dengan iklan untuk Viagra, iklan untuk tarif hipotek rendah, promosi untuk berbagai saham, dan pengungsi Nigeria yang membutuhkan bantuan mendapatkan \$ 30.000.000 di luar Afrika. Beberapa spammer menyamarkan alamat pengirim mereka sehingga memantul email dari akun yang tertutup atau tidak sah. Spamming untuk pencurian identitas: Bagian 5.3

tidak mengganggu mereka. ISP menyaring email dari spammer yang dikenal, sehingga banyak yang menyamarkan sumbernya dan menggunakan skema lain untuk menghindari filter. Spammer kriminal membajak sejumlah besar komputer dengan menyebarkan virus yang memungkinkan spammer mengirim spam dalam jumlah besar dari mesin yang terinfeksi, yang disebut "zombies." Berapa banyak spam yang melewati Internet? Kasus pertama yang menciptakan kehebohan antispam yang melibatkan pesan-pesan iklan yang dikirim oleh firma hukum ke 6000 papan buletin atau grup berita pada tahun 1994. Pada saat itu, setiap iklan atau posting yang tidak secara langsung terkait dengan topik kelompok itu membangkitkan kemarahan pengguna Net. Baru-baru ini, seorang pria dituduh menjalankan jaringan zombie yang mengirim miliaran email per hari. Spammer lain ditangkap karena menyumbat Facebook dengan 27 juta pesan spam.²⁷

Mengapa tidak hanya melarang spam? Kami akan melihat beberapa alasan dalam beberapa halaman berikutnya.

y Spam adalah nama produk daging yang dibumbui yang dijual dalam kaleng oleh Hormel Foods. Penggunaan kata dalam konteks email berasal dari sandiwara Monty Python di mana beberapa karakter berulang kali berteriak, "Spam, spam, spam," menenggelamkan percakapan lain.

Kasus dan masalah kebebasan berbicara

Pada tahun 1996, sekitar setengah dari email yang diterima di AOL adalah spam, dan banyak dari itu berasal dari layanan periklanan email yang disebut Promosi Cyber. AOL memasang filter untuk memblokir email dari Promosi Cyber. Promosi Cyber memperoleh perintah terhadap penggunaan filter AOL, mengklaim AOL melanggar hak Amendemen Pertama. Maka dimulailah pertarungan atas status hukum spam.

Kasus Cyber Promotions lemah, dan pengadilan segera menghapus perintah. Mengapa AOL berhak memblokir spam yang masuk? Spam menggunakan komputer AOL, membebankan biaya pada AOL. Hak milik AOL memungkinkannya memutuskan apa yang diterima di sistemnya. AOL adalah organisasi keanggotaan; ia dapat menerapkan kebijakan untuk menyediakan jenis lingkungan yang diyakini para anggotanya inginkan. Akhirnya, AOL adalah perusahaan swasta, bukan lembaga pemerintah. Di sisi lain, beberapa organisasi kebebasan sipil merasa tidak nyaman karena mengizinkan AOL untuk memfilter email karena AOL memutuskan email apa yang diblokir dari anggotanya. Mereka berpendapat bahwa karena AOL besar, sangat mirip dengan Kantor Pos, dan seharusnya tidak diizinkan untuk memblokir email apa pun.

Selama beberapa tahun ke depan, AOL mengajukan beberapa tuntutan hukum dan meminta perintah untuk menghentikan pengirim spam mengirim surat massal yang tidak diminta ke anggotanya. Perhatikan pergeseran halus: Promosi Cyber mencari perintah untuk menghentikan AOL agar tidak memfilter emailnya. AOL meminta perintah untuk menghentikan pengirim spam mengirim email. Filter tidak melanggar kebebasan berbicara spammer, tetapi apakah perintah untuk tidak mengirim surat melanggar kebebasan berbicara? Kami mencantumkan beberapa argumen mengapa penyedia layanan harus bebas menyaring email masuk. Apakah ada argumen yang mendukung perintah terhadap spammer? Salah satunya: argumen bahwa spam menggunakan properti perusahaan penerima (sistem komputer) terhadap keinginannya dan membebankan biaya pada penerima. AOL dan layanan lainnya memenangkan pemukiman jutaan dolar dari Promosi Cyber dan spammer lainnya. Tetapi seberapa jauh, atau seharusnya, kendali pemiliknya meluas? Seorang mantan karyawan Intel, Ken Hamidi, memelihara situs web yang kritis terhadap Intel. Dia mengirim enam email kepada lebih dari 30.000 karyawan Intel selama periode kurang dari dua tahun. Dia menyamakan alamat pengirimnya, menyulitkan Intel untuk memblokir emailnya. Intel mencari perintah pengadilan yang melarangnya mengirim lebih banyak email ke karyawannya (di tempat kerja). Perhatikan bahwa dalam hal ini spam tidak bersifat komersial. Intel berpendapat bahwa kebebasan berbicara memberi Hamidi hak untuk mengoperasikan situsnya sendiri, tetapi itu tidak memberinya hak untuk mengganggu properti Intel dan menggunakan peralatannya untuk menyampaikan pesan-pesannya. Intel berpendapat bahwa email itu adalah bentuk pelanggaran. Mahkamah Agung California memutuskan mendukung Hamidi. Pengadilan mengatakan bahwa email massal Hamidi bukanlah pelanggaran, karena tidak merusak komputer Intel atau menyebabkan kerugian ekonomi bagi perusahaan. Para hakim yang tidak setuju berpendapat bahwa hak milik Intel atas komputernya harus memungkinkan perusahaan untuk mengecualikan email yang tidak diinginkan.²⁸

Amnesty International telah lama menggunakan jaringan ribuan relawannya untuk membanjiri pejabat pemerintah di berbagai negara dengan surat ketika tahanan politik disiksa atau dalam bahaya eksekusi. Misalkan sebuah organisasi mengirimsama

Masalah untuk desainer dan pengguna filter

Kami melihat bahwa filter tidak sempurna. Mereka memblokir lebih atau kurang dari materi yang ingin diblokir, dan sering mereka memblokir lebih dan kurang. Jika filter dimaksudkan untuk memblokir materi seksual yang eksplisit dari anak-anak kecil, mungkin dapat diterima untuk melakukan kesalahan di sisi memblokir beberapa bahan inoffensive untuk memastikan mencegah bahan yang tidak diinginkan untuk lolos. Di sisi lain, jika filter adalah untuk spam, kebanyakan orang tidak keberatan beberapa pesan spam berhasil tetapi akan sangat tidak senang jika beberapa email nonspam mereka dibuang.

email ke setiap anggota Kongres (atau ke daftar bisnis) setiap kali seseorang mengunjungi situs tersebut dan mengklik untuk mengirimkannya. Akankah kita memiliki sudut pandang yang berbeda tentang apakah ini kebebasan berbicara atau spam, tergantung pada seberapa bersimpati kita terhadap pesan organisasi tertentu?

Mengurangi masalah spam

Kebebasan berbicara tidak mengharuskan pendengar yang dimaksudkan, atau penerima pesan, untuk mendengarkan. Bisnis dan programmer menciptakan berbagai produk penyaringan untuk menyaring spam di situs penerima, dengan memblokir email dari alamat tertentu, dengan memblokir pesan dengan kata-kata tertentu, dan dengan metode yang lebih canggih. Banyak orang sekarang melihat sangat sedikit spam karena penyedia layanan email mereka menyaringnya.

Banyak perusahaan berlangganan layanan yang menyediakan daftar spammer untuk diblokir. Daftar layanan antispam yang agresif tidak hanya spammers tetapi juga ISP, universitas, bisnis, dan layanan online yang tidak mengambil tindakan yang cukup untuk menghentikan anggota komunitas mereka mengirim spam. Tindakan semacam itu mendorong para manajer untuk melakukan sesuatu — misalnya, membatasi jumlah pesan keluar dari satu akun. Berapa banyak kebijaksanaan yang harus dimiliki oleh layanan antispam dalam memutuskan siapa yang harus dimasukkan dalam daftar spammernya? Harris Aktifitas, yang melakukan survei opini publik melalui email ("jajak pendapat Harris"), menggugat Sistem Pencegahan Penyalahgunaan Mail (MAPS) untuk memasukkan Harris dalam daftar hitamnya. Harris mengklaim bahwa orang yang menerima emailnya mendaftar untuk menerimanya. MAPS mengklaim Harris tidak memenuhi standar untuk memastikan persetujuan penerima. Harris mengklaim sebuah perusahaan pemungutan suara yang bersaing merekomendasikannya untuk daftar spammer.²⁹ Harris mengklaim dimasukkan dalam daftar itu memotongnya dari sekitar separuh peserta survei dan merusak bisnisnya. Kasus ini mengilustrasikan potensi untuk "bermain" sistem oleh pesaing dan perbedaan pendapat yang dapat timbul tentang siapa yang menjadi spammer.

Sangat menarik untuk meninjau bagaimana sikap tentang penyaringan spam telah berubah. Kami melihat bahwa ketika AOL mulai memfilter secara agresif untuk memblokir spam, beberapa grup internet membandingkan pemfilteran dengan penyensoran. Meskipun AOL bukan entitas pemerintah, itu besar dan jutaan orang menerima surat mereka di AOL. Orang-orang khawatir bahwa preseden

dari perusahaan besar yang memfilter email karena alasan apa pun dapat menyebabkan perusahaan memfilter email karena konten yang tidak mereka sukai. Sekarang, banyak kelompok advokasi dan pelanggan layanan komunikasi melihat penyaringan spam sebagai hal yang berharga dan penting.

Spam itu murah. Jadi, ide lain untuk mengurangi itu adalah meningkatkan biayanya ke pengirim. Proposal mencakup skema email dan skema tersertifikasi di mana pengirim email membayar sedikit biaya kepada penerima untuk setiap pesan email yang mereka kirim. Untuk email yang disertifikasi, pengesah akan memeriksa pengirim yang mendaftar ke layanan dan, dengan sedikit biaya per pesan, menyatakan bahwa surat mereka bukan spam. Pengesah membuat perjanjian dengan ISP dan penyedia layanan email bahwa mereka mengirimkan surat tersertifikasi ke anggota, gambar, dan tautan mereka, tanpa meletakkan filter melalui email. Pesan-pesan itu muncul di kotak surat penerima dengan indikasi bahwa pesan-pesan itu "tersertifikasi."

Banyak kelompok keberatan dengan gagasan untuk membebaskan biaya apa pun untuk mengirim email. Sebagai contoh, Richard Cox dari Spamhaus, sebuah organisasi antispam internasional, berkomentar bahwa "muatan e-mail akan menghancurkan semangat Internet." 30 Kritikus mengatakan biaya mungkin mengurangi penggunaan email oleh orang miskin dan organisasi nirlaba. Kritik terhadap skema surat tersertifikasi, seperti Spamhaus dan Electronic Frontier Foundation, percaya bahwa mereka memberikan insentif kepada ISP untuk tidak meningkatkan filter, terutama jika penyedia layanan mendapatkan bagian dari biaya sertifikasi. ISP juga akan memiliki insentif untuk melakukan overfilter — yaitu, menyaring email yang sah sehingga lebih banyak pengirim harus membayar untuk sertifikasi.

Hukum antispam Dampak hukum dan keputusan antispam tentang konstitusionalitas mereka bisa sangat signifikan. Seorang pria yang dihukum karena melakukan spam di Virginia dijatuhi hukuman sembilan tahun penjara. Hukum Virginia melarang anonim, tidak diminta, email massal. Keyakinan itu terbalik ketika Mahkamah Agung negara memutuskan bahwa hukum melanggar Amandemen Pertama. UU CAN-SPAM federal³¹ berlaku untuk email yang dikirim ke komputer dan perangkat seluler. Ini menargetkan spam komersial dan mencakup pelabelan pesan iklan (untuk mempermudah penyaringan), ketentuan penyisihan, dan metode pembuatan daftar email. Pesan komersial harus menyertakan informasi header surat yang valid (yaitu memalsukan "Dari" garis untuk menyamarkan pengirim dilarang) dan alamat pengirim yang valid. Baris subjek yang menipu dilarang. Hukuman pidana berlaku untuk beberapa praktik yang lebih menipu dan untuk mengirimkan spam dari komputer orang lain tanpa otorisasi (sebuah proses yang dapat diselesaikan oleh virus yang mengambil alih komputer lain) .³² Dalam aplikasi hukum pertama, empat orang dituduh mengirimkan penawaran penjualan untuk produk penurunan berat badan palsu dan menyamarkan identitas mereka.

Banyak organisasi antispam yang menentang UU CAN-SPAM karena mereka lebih suka melihat spam yang dilarang sama sekali (seperti di beberapa negara), bukannya dilegitimasi oleh peraturan. Banyak bisnis yang didukung CAN-SPAM. Undang-undang telah membantu mengurangi masalah spam dari bisnis yang sah. Kita bisa menyaringnya dan kita bisa keluar dari milis. Orang-orang yang mengirim spam yang menyertakan skema penipuan "cepat kaya" atau iklan untuk pornografi anak jelas tidak peduli dengan apa yang legal. Mereka tidak mungkin

3.3 Memposting, Menjual, dan Membocorkan Materi Peka 152

mematuhi hukum untuk mengidentifikasi diri mereka. Undang-undang semacam itu mempermudah untuk mendenda atau memenjarakan mereka dengan menghukum mereka melanggar peraturan antispam dalam kasus-kasus di mana tidak ada bukti yang cukup untuk keyakinan berdasarkan isi pesan. Apakah ini manfaat atau ancaman terhadap kebebasan berbicara dan proses hukum?

Spammer terus menemukan cara baru di sekitar pemblokir spam. Kesulitan membedakan spam dari surat nyata dengan kepastian mutlak menunjukkan bahwa siklus teknik spam baru dan teknik pemblokiran yang lebih baik akan terus berlanjut. Karena undang-undang antispam harus menghindari konflik dengan kebebasan berbicara, dan karena pelaku spam yang paling kasar mengabaikan undang-undang, hukum dapat mengurangi spam tetapi tidak mungkin menghilangkan masalah.

3.2.5 Menantang Struktur Peraturan Lama dan Minat Khusus

Kebanyakan orang tidak akan mempertimbangkan iklan untuk anggur dan real estate di Web sebagai materi yang menyinggung. Namun, kelompok minat khusus mencoba menghapusnya. Kelompok-kelompok semacam itu melobi (seringkali berhasil) untuk undang-undang untuk membatasi penggunaan teknologi baru yang mereka anggap sebagai ancaman terhadap pendapatan dan pengaruh mereka. Sebagian besar kasus yang kita diskusikan di sini memiliki implikasi ujaran bebas. Beberapa melibatkan peraturan hukum yang membatasi iklan dan penjualan di Web. Peraturan seperti itu memiliki tujuan mulia, seperti melindungi masyarakat dari penipuan. Mereka juga memiliki pengaruh membudaya yang sudah kuat, menjaga harga tinggi, dan membuatnya lebih sulit bagi bisnis baru dan kecil atau suara independen untuk berkembang.

Beberapa perusahaan menjual perangkat lunak self-help untuk membantu orang dalam menulis surat wasiat, perjanjian pra-pernikahan, dan banyak dokumen hukum lainnya. Perangkat lunak ini mencakup formulir dan instruksi hukum untuk mengisinya. Ini adalah contoh khas memberdayakan orang biasa dan mengurangi ketergantungan kita pada ahli yang mahal. Seorang hakim Texas melarang perangkat lunak hukum Quicken dari Texas dengan argumen bahwa perangkat lunak berjumlah untuk mempraktekkan hukum tanpa lisensi Texas. Badan legislatif Texas kemudian mengubah hukumnya untuk membebaskan penerbit perangkat lunak.

Ketika orang mulai menerbitkan buletin online tentang jenis investasi tertentu, mereka menemukan bahwa mereka melanggar peraturan berusia 25 tahun yang membutuhkan lisensi pemerintah. Persyaratan lisensi termasuk biaya, sidik jari, pemeriksaan latar belakang, dan menyajikan daftar pelanggan sesuai permintaan ke Komisi Perdagangan Berjangka Komoditas (CFTC), agen federal yang mengelola peraturan. Penerbit yang tidak mendaftar dengan CFTC dapat didenda hingga \$ 500.000 dan dipenjara hingga lima tahun. Peraturan itu dirancang untuk pedagang yang menangani uang orang lain, tetapi CFTC menerapkannya kepada orang yang menjual buletin atau perangkat lunak investasi untuk menganalisis pasar komoditas berjangka. Seorang hakim federal memutuskan bahwa peraturan CFTC adalah pengekangan sebelumnya pada pidato dan melanggar Amandemen Pertama baik untuk penerbit Internet dan penerbit surat kabar tradisional. Dengan mengangkat isu kebebasan berbicara di Web, kasus ini menyebabkan

y gangster Larangan-era Al Capone masuk penjara karena penghindaran pajak karena jaksa tidak bisa menghukumnya atas kejahatan lain.

3.3 Memposting, Menjual, dan Membocorkan Materi Peka 153

untuk menghentikan pembatasan bebas bicara yang tidak konstitusional dalam media tradisional.³³

Web menyediakan potensi untuk menurunkan harga untuk banyak produk dengan menghilangkan “perantara”. Produsen kecil, yang tidak mampu membeli distributor mahal atau pedagang grosir, dapat menjual langsung ke konsumen di seluruh negeri. Tetapi tidak jika bisnis itu adalah anggur kecil. Tiga puluh negara bagian di AS memiliki undang-undang yang melarang pengiriman anggur di luar negara secara langsung kepada konsumen. Undang-undang melindungi bisnis grosir besar yang biasanya mendapatkan 18% -25% dari harga dan membeli sebagian besar dari perkebunan anggur besar atau yang menjual anggur mahal. Undang-undang juga melindungi penerimaan negara; pemerintah negara bagian tidak dapat mengumpulkan pajak penjualan atas banyak penjualan di luar negara bagian. Pemerintah negara bagian berpendapat bahwa undang-undang mencegah penjualan kepada anak di bawah umur. Ini adalah argumen lemah di negara yang mengizinkan pengiriman langsung dari kilang anggur di negara bagian. New York juga melarang iklan anggur out-of-state langsung ke konsumen di negara bagian. Sebuah kilang anggur yang mengiklankan anggurnya di Web berisiko karena situs web dapat diakses oleh konsumen di New York. Operator-operator anggur menantang undang-undang anggur New York, dengan alasan bahwa itu secara tidak terbatas membatasi kebebasan berbicara, mengganggu perdagangan antar negara bagian, dan mendiskriminasi bisnis di luar negara.³⁴ Mahkamah Agung memutuskan bahwa larangan pengiriman barang keluar-langsung kepada konsumen tidak konstitusional.

Pemerintah California dan New Hampshire berusaha untuk mewajibkan para operator situs web seperti ForSaleByOwner.com mendapatkan lisensi real estat negara bagian di negara bagian tersebut karena mereka mencantumkan rumah yang dijual di negara bagian. Persyaratan lisensi tidak relevan dan mahal untuk situs semacam itu, dan undang-undang negara mengizinkan surat kabar untuk menerbitkan iklan real estat, baik di koran itu sendiri maupun di situs web mereka, tanpa lisensi real estat. Pengadilan federal memutuskan bahwa persyaratan untuk lisensi real estate ini melanggar hak Amandemen Pertama dari operator situs web. Keputusan tersebut melindungi hak Amandemen Pertama yang sama untuk situs web sebagaimana untuk media yang lebih lama dan juga mengurangi kekuatan dari suatu kepentingan khusus (dalam hal ini, broker real estate) untuk membatasi persaingan.

Di Prancis, tarif pajak pada e-buku adalah 19,6%. Pajak atas buku cetak adalah 5,5%. Sebuah undang-undang di Prancis melarang toko memberikan diskon besar pada buku cetak. Penjual buku kecil meminta pemerintah Prancis untuk peraturan serupa untuk ebooks. Ketika saya menulis ini, pemerintah Prancis berencana untuk mengurangi pajak ebook tetapi menunda pengurangan. Mungkin popularitas ebooks dan diskon akan menyebabkan pembalikan dari undang-undang lama yang membatasi diskon buku cetak.

3.3 Memposting, Menjual, dan Membocorkan Materi Sensitif

Pidato bebas ditingkatkan oleh kesopanan.

—Tim O'Reilly 35

Sebagian besar diskusi kita sejauh ini terfokus pada hukum penyensoran, undang-undang yang melarang distribusi atau akses ke jenis materi tertentu. Materi hukum yang dapat menjadi sensitif dalam beberapa hal.

menimbulkan masalah sosial dan etika. Contohnya termasuk materi hiburan "dewasa" yang sah, materi Nazi, informasi pribadi tentang orang lain, dan peta serta informasi lain yang mungkin berguna bagi teroris. Penerbitan yang disengaja dari materi sensitif yang bocor (mungkin dicuri) untuk tujuan politik atau sosial menimbulkan masalah sosial dan etika (serta masalah hukum). Di bagian ini, kami mempertimbangkan beberapa di antaranya.

Kebijakan perusahaan besar

Pembalikan kebijakan oleh beberapa situs web besar mengilustrasikan beberapa dilema tentang memposting materi hukum yang menyinggung banyak orang. Ketika Yahoo memperluas toko onlinenya untuk materi dewasa (erotika, video seks, dan sebagainya — semuanya legal), banyak pengguna yang mengeluh. Kritikus keberatan karena Yahoo adalah perusahaan besar dan besar, aksinya memberi akseptabilitas terhadap pornografi. Yahoo membalik kebijakan dan menghapus iklan untuk materi khusus dewasa. Ini membawa keluhan dari orang lain bahwa perusahaan "menyerah" terhadap tekanan dari pengiklan dan pengguna utamanya. Beberapa orang percaya bahwa itu salah untuk bisnis besar yang berpengaruh, seperti Google, Craigslist, Amazon, atau Yahoo, misalnya, untuk melarang materi hukum apa pun dari layanannya karena efeknya mirip dengan sensor pemerintah.

Berbagai perusahaan online memiliki kebijakan yang menentang pengeposan materi kebencian, informasi pembuatan bom, dan materi yang tidak menyenangkan atau berisiko lainnya. Apple menolak aplikasi ponsel pintar yang dianggapnya tidak pantas; itu tidak akan menjualnya di app store-nya. Banyak situs lelang melarang penjualan beberapa jenis produk hukum. Pengecer besar membatasi penjualan untuk anak-anak di bawah umur dari gim video dengan kekerasan, ketelanjangan, dan seks. Apakah hak hukum orang dewasa untuk membeli atau membaca sesuatu (hak negatif, untuk bebas dari penangkapan) memberlakukan kewajiban etis atau sosial pada bisnis untuk menyediakannya? Pembeneran utama untuk jawaban afirmatif adalah, seperti yang disebutkan di atas, menyamakan dampak sosial besar dari perusahaan besar dengan sensor. Di sisi lain, dalam masyarakat yang bebas di mana pemerintah tidak memutuskan apa yang bisa kita baca atau lihat, lebih penting bagi penjual dan individu untuk secara serius memerhatikan peran dan tanggung jawab mereka dalam memutuskan bahan apa yang akan mereka sediakan. Juga, perusahaan swasta memiliki hak properti dalam bisnisnya yang mencakup pengambilan keputusan tentang apa yang harus dijual. Jika sebagian besar masyarakat menganggap beberapa materi tidak pantas untuk situs web dan toko utama, maka respons terhadap tekanan pelanggan mungkin akan menjauhkannya dari tempat-tempat tersebut. Ini masih akan tersedia dari situs khusus dan dealer.

Bagaimana dengan penyedia mesin telusur? Apakah mereka memiliki kewajiban sosial atau etika untuk memberikan hasil pencarian lengkap untuk semua pertanyaan, atau apakah mereka memiliki kewajiban sosial atau etika untuk menghilangkan situs yang sangat menyinggung dari hasil pencarian? Orang-orang yang menetapkan kebijakan di perusahaan seperti itu menghadapi pertanyaan sulit. Bagaimana seharusnya mesin pencari menanggapi pencarian "foto telanjang mahasiswa"? Bagaimana seharusnya menanggapi pencarian gambar-gambar penyiksaan grafis oleh pemerintah atau oleh teroris? Mesin pencari menyediakan layanan yang sangat berharga dan mendasar. Kami tidak ingin mereka mendiskriminasi opini yang tidak populer atau sebagian besar bentuk materi kontroversial. Kami ingin mencari berita dan, terkadang, fakta yang tidak menyenangkan. Namun pengakuan penggunaan beberapa bahan antisosial atau berisiko dapat menyebabkan keputusan etis untuk menolak untuk menyajikannya secara jelas, atau sama sekali.

Situs web dengan risiko

Pertimbangkan situs web yang mungkin dibuat oleh organisasi individu atau kecil. Untuk membuat beton diskusi, kami mempertimbangkan sebuah situs tentang bunuh diri untuk pasien yang sakit parah dengan rasa sakit yang konstan dan berat. Poin yang kami angkat di sini berlaku untuk jenis informasi sensitif lainnya juga. Apa yang harus dipertimbangkan oleh penyelenggara situs? Pertama, meskipun situs tersebut tidak diiklankan, mesin pencari akan menemukannya. Remaja yang depresi dan orang dewasa yang depresi akan menemukannya. Apa yang kami tempatkan di situs web publik bersifat publik, tersedia untuk semua orang di seluruh dunia. Penyelenggara harus memikirkan risiko potensial dan menelitinya. Lalu apa? Salah satu pilihan adalah memutuskan untuk tidak mengatur situs sama sekali. Misalkan penyelenggara situs memutuskan untuk melanjutkan karena mereka percaya rencana mereka memiliki nilai yang signifikan untuk audiens yang dituju. Apa yang bisa mereka lakukan untuk mengurangi risiko? Mungkin memerlukan kata sandi untuk mengakses situs. Bagaimana seseorang mendapatkan kata sandi? Apakah periode menunggu yang sederhana akan mengurangi risiko orang yang mengalami depresi sementara? Apakah persyaratan kata sandi mencegah akses oleh pengguna yang dituju karena masalah privasi? Apakah Anda memiliki tanggung jawab etis untuk menghindari membantu anak berusia 15 tahun bunuh diri? Dapatkah Anda menganggap mereka akan menemukan informasi untuk melakukannya di tempat lain dan bahwa tanggung jawab untuk memutuskan adalah milik mereka? Apakah Anda memiliki tanggung jawab etis untuk membantu orang yang sakit parah kesakitan untuk bunuh diri? Atau apakah situs Anda menawarkan layanan yang diinginkan sebagian orang tetapi dengan risiko kepada orang lain yang Anda perlu meminimalkan?

Orang yang memposting materi berisiko memiliki tanggung jawab etis untuk secara serius mempertimbangkan pertanyaan seperti ini. Jawabannya terkadang tidak jelas atau mudah. Kebebasan berbicara bukanlah faktor penentu.

Entah memikirkan tentang menyiapkan situs web dengan informasi sensitif atau memikirkan untuk menyampaikan video yang lucu tetapi memalukan dari seorang teman, kami merangkum beberapa panduan: Pertimbangkan potensi risiko. Pertimbangkan pembaca atau pengguna yang tidak diinginkan. Pertimbangkan cara untuk mencegah akses oleh pengguna yang tidak diinginkan. Ingat bahwa mungkin sulit untuk menarik materi setelah dilepaskan.

Kebocoran Web

Kebocoran web adalah alat yang nyaman dan kuat untuk pelapor. Orang dapat secara anonim memposting dokumen dan membuatnya tersedia bagi dunia. Organisasi kecil dan perusahaan berita besar membuat situs khusus untuk menerima dan mempublikasikan dokumen yang bocor. Korupsi dan penyalahgunaan kekuasaan dalam bisnis dan pemerintah adalah topik umum. Beberapa kebocoran melayani tujuan sosial yang berharga. Di sisi lain, karena mudah bocornya cache besar dokumen orang lain, orang terkadang melakukannya dengan sembarangan. Materi sensitif, bocor tidak bertanggung jawab, dapat membahayakan orang yang tidak bersalah.

Sepanjang, kita harus ingat bahwa bocor dimulai dengan kasus etis yang kuat terhadapnya. Dokumen yang bocor sering diperoleh dengan meretas ke komputer orang lain atau oleh orang dalam yang melanggar perjanjian kerahasiaan. Dokumen-dokumen milik

y Beberapa orang menganggap bunuh diri itu sendiri, dan dorongan apapun dari itu, menjadi tidak bermoral. Demi diskusi ini, kami menganggap orang-orang yang mengatur situs tidak.

3.3 Memposting, Menjual, dan Membocorkan Materi Sensitif 156

seseorang; mereka dicuri atau digunakan tanpa izin pemilik. Kebocoran dapat menyebabkan kerusakan serius pada seseorang atau organisasi tanpa mereka melakukan sesuatu yang salah. Kebebasan berbicara dan pers tidak sah mencuri file dan menerbitkannya, juga tidak beralasan bertindak tidak bertanggung jawab. Ini tidak berarti bahwa bocor selalu salah. Ini berarti bahwa alasan untuk membocorkan materi harus cukup kuat untuk mengatasi argumen etis terhadapnya, dan penerbit bahan yang bocor harus menanganinya secara bertanggung jawab.

Untuk menganalisis etika kebocoran tertentu, kami mempertimbangkan jenis materi yang dirilis, nilai bagi masyarakat, dan risiko bagi masyarakat dan individu yang tidak bersalah. Kami juga melihat masalah tambahan terkait dengan rilis dokumen dalam jumlah sangat besar dan beberapa tanggung jawab siapa pun yang mengatur situs untuk menerima dan mempublikasikan materi yang bocor.

Dokumen yang mencakup bukti signifikan dari kesalahan serius adalah kandidat yang layak untuk kebocoran. Keliru bisa jadi korupsi; represi politik; pembunuhan massal oleh tentara dalam perang internasional (atau internal); pelanggaran serius terhadap hukum atau etika profesional; penyimpangan keamanan dalam sistem besar yang mempengaruhi publik; praktik tidak jujur oleh pengusaha, ilmuwan, atau polisi; dan menutup-nutupi kegiatan semacam itu — untuk mengutip hanya beberapa kategori. Kelas dokumen lain menggambarkan diskusi internal dan pengambilan keputusan dalam bisnis, organisasi, atau pemerintah, dan laporan yang jujur tentang produk dan acara. Ada pembenaran untuk membocorkan ini jika mereka memberikan bukti kesalahan atau risiko, tetapi tidak hanya untuk mempermalukan orang atau merusak pesaing atau organisasi yang tidak disetujui. Dalam diskusi ini, kami menggunakan dua contoh kontroversial yang terlalu luas dan rumit untuk dianalisis sepenuhnya di sini. Mereka membantu mengilustrasikan pertanyaan-pertanyaan yang perlu dipertimbangkan ketika mengevaluasi kebocoran, dan — saya harap — mereka menghasilkan lebih banyak diskusi. Salah satunya adalah set besar dokumen militer dan diplomatik AS yang dibuat WikiLeaks publik. Yang lain, kadang-kadang disebut "Climategate," adalah kumpulan email dan dokumen lain dari Unit Penelitian Iklim di University of East Anglia di Inggris, salah satu dari pusat utama penelitian tentang pemanasan global.

Email Climategate bocor pada tahun 2009 dan 2011 menunjukkan bahwa para peneliti di University of East Anglia mengejar berbagai metode untuk menolak akses ke data suhu mereka oleh para ilmuwan yang mempertanyakan beberapa aspek pemanasan global. Menolak akses ke data adalah pelanggaran praktik ilmiah. Email tersebut juga menggambarkan upaya untuk menghentikan jurnal ilmiah dari penerbitan makalah oleh para ilmuwan yang dianggap skeptis tentang pemanasan global dan untuk menyerang reputasi beberapa ilmuwan tersebut. Investigasi oleh pemerintah Inggris dan kelompok lain menyimpulkan bahwa email tidak menunjukkan kesalahan ilmiah, tetapi pusat penelitian telah melanggar Undang-undang Kebebasan Informasi Inggris. Laporan tersebut mengkritik berbagai prosedur yang digunakan kelompok riset tetapi bukan kesimpulan ilmiahnya. Beberapa email membahas kritik dan ketidakpastian terkait dengan detail dari argumen bahwa aktivitas manusia menyebabkan pemanasan global. Para peneliti mendiskusikan ketidakpastian seperti itu

Sebelumnya, banyak materi WikiLeaks yang dibuat publik sesuai kriteria masuk akal untuk kebocoran yang dapat dibenarkan, atau dikagumi. Contohnya termasuk dokumen yang mengekspos korupsi di berbagai pemerintah dan mengekspos pembunuhan oleh polisi di Kenya.

ikatan dalam makalah dan konferensi, tetapi laporan berita sering mengecualikannya. Apakah penting bagi publik untuk mengetahui apa yang ada di email? Kriteria apa yang mendukung atau menentang kebocoran ini? 36 WikiLeaks merilis dokumen militer AS terkait dengan perang di Irak dan Afghanistan, termasuk video insiden penembakan. Ketika perang yang panjang dan mahal kontroversial, apakah publik memiliki hak untuk melihat laporan internal dan video yang jelas yang dapat menginformasikan perdebatan? Wikileaks merilis satu set besar kabel diplomatik AS rahasia yang termasuk, di antara yang lainnya, diskusi tentang kepribadian para pemimpin asing. Apakah nilai menginformasikan kepada publik lebih besar daripada nilai diskusi internal yang rahasia dan jujur ketika mengembangkan kebijakan diplomatik?

Ketika mengevaluasi etika dokumen yang bocor pada isu-isu politik atau sangat dipolitisir, bisa sulit untuk membuat penilaian yang independen dari pandangan kita tentang isu-isu itu sendiri. Beberapa orang percaya bahwa penilaian kita tentang kebocoran tidak boleh terlepas dari masalah: Jika kita menentang kebijakan luar negeri AS, kebocoran WikiLeaks adalah baik. Jika kita skeptis tentang pemanasan global, kebocoran penelitian iklim itu baik. Tentu saja, jika kita berpegang pada pandangan yang berlawanan, kita dapat mengevaluasi kebocorannya secara berlawanan. Ini tidak membantu kami mengembangkan kriteria yang baik untuk mengevaluasi etika bocor dan membimbing kami jika kami memiliki akses ke data sensitif. Kita dapat membuat kasus yang lebih kuat untuk kriteria etis yang dapat digunakan untuk mengevaluasi kebocoran jika kita bersedia menerapkan kriteria yang sama untuk membocorkan materi serupa di kedua sisi masalah politik.

Kebocoran yang berpotensi berbahaya

WikiLeaks merilis sebuah situs daftar kritis pemerintah rahasia AS, seperti telekomunikasi hub, bendungan, saluran pipa, pasokan mineral penting, kompleks manufaktur, dan sebagainya, di mana kerusakan atau gangguan akan menyebabkan bahaya yang signifikan. Beberapa mungkin membela publikasi daftar tersebut dengan menyatakan bahwa hal itu mendorong perlindungan situs yang lebih baik atau bahwa teroris sudah tahu tentang situs, tetapi risikonya tampaknya membanjiri nilai publik dari kebocoran ini. Dokumen-dokumen lain diskusi rinci antara pejabat pemerintah AS dan pemimpin oposisi di negara dengan pemerintah yang sangat represif. Beberapa kabel bernama whistleblower, informan rahasia, aktivis hak asasi manusia, petugas intelijen, dan orang Cina (dalam bisnis, akademisi, dan pemerintah Cina) yang memberikan informasi tentang kondisi sosial dan politik di Tiongkok. Pelepasan dokumen-dokumen ini menempatkan orang-orang itu dalam bahaya. Dokumen-dokumen lain menyebut orang-orang yang melarikan diri dari negara-negara yang represif, berpotensi membahayakan keluarga mereka. Beberapa kebocoran tidak membahayakan nyawa, tetapi mereka melanggar privasi atau mengancam pekerjaan, reputasi, kebebasan, dan nilai-nilai lainnya. Mereka yang menyediakan materi dan mereka yang mempublikasikannya memiliki tanggung jawab etis untuk menghindari atau meminimalkan merugikan orang yang tidak bersalah.³⁷

y Ada indikasi bahwa nama-nama dihapus dalam beberapa kasus. Pembocoran email Climategate menggunakan perangkat lunak otomatis untuk menghapus informasi kontak pribadi dan informasi pribadi lainnya di email (meskipun beberapa tetap, menurut beberapa laporan).

Melepaskan sekumpulan besar dokumen

Dokumen pemerintah AS yang dibuat WikiLeaks dipublikasikan termasuk sekitar 250.000 kabel diplomatik dan ribuan dokumen lainnya. The Climatedge kebocoran termasuk ribuan dokumen. Apakah leakers meninjau dan mengevaluasi semua dokumen yang mereka rilis untuk memastikan mereka memenuhi kriteria yang masuk akal untuk membenarkan kebocoran? Haruskah mereka memilikinya? Dalam semangat Web, leakers sekarang dapat membiarkan pencarian publik melalui dokumen-dokumen untuk kepentingan khusus. Ini bisa berharga, tetapi bisa salah. Ingat bahwa pembenaran penting untuk membocorkan dokumen milik orang lain adalah bahwa leaker tahu mereka mengandung informasi yang harus dilihat publik. Jika sebagian besar informasi tidak memenuhi kriteria untuk kebocoran etika, maka mungkin sulit untuk membenarkan penerbitan seluruh rangkaian dokumen. Dokumen-dokumen itu mungkin menarik bagi publik, tetapi dalam banyak kasus itu tidak cukup pembenaran. Di sisi lain, pengungkapan selektif dapat mendistorsi informasi dengan menyajikannya tanpa konteks. Pilihan terbaik mungkin tidak mudah.

Privasi dan kerahasiaan penting bagi individu dan fungsi yang sah dari bisnis dan pemerintah. Privasi dan kerahasiaan bukanlah hak mutlak, tetapi itu adalah nilai yang signifikan. Leaker memiliki banyak tanggung jawab etis untuk menghormati privasi (bahkan untuk orang yang tidak mereka sukai atau tidak sependapat) seperti yang dilakukan pemerintah dan bisnis. Dengan demikian, pembenaran untuk mengesampingkan privasi dan penerbitan dokumen rahasia harus kuat dan cukup spesifik.

Bocornya dokumen pemerintah adalah kasus khusus. Dalam beberapa hal lebih dapat dibenarkan untuk membocorkan atau mempublikasikan dokumen pemerintah; dengan cara lain kurang dapat dibenarkan. Publik memiliki klaim yang wajar atas hak untuk mengetahui apa yang sedang dilakukan atas namanya dan dengan uangnya. Di sisi lain, investigasi kriminal dan keamanan nasional sering membutuhkan kerahasiaan. Banyak negara bagian dan negara-negara bebas memiliki undang-undang yang mengharuskan pengungkapan catatan publik tertentu dan undang-undang seperti Undang-Undang Kebebasan Informasi yang memungkinkan akses publik ke catatan pemerintah dalam banyak situasi. Proses hukum dapat menjadi membosankan dan tidak efektif kadang-kadang, tetapi proses harus dicoba, jika mereka berlaku, sebelum beralih ke peretasan untuk mendapatkan file atau memperolehnya dari orang dalam. Terkadang, kebocoran bisa menjadi satu-satunya cara untuk membongkar korupsi dan menutup-nutupi.

Tanggung jawab operator situs web untuk kebocoran

Misalkan seseorang atau organisasi memutuskan untuk membuat situs untuk mempublikasikan dokumen yang bocor yang melayani tujuan publik yang penting. Selain memberikan pertimbangan serius terhadap berbagai poin yang kami ajukan, operator situs memiliki tanggung jawab untuk menghindari penyalahgunaan situs. Situs ini harus memiliki keamanan yang cukup untuk melindungi para pelapor — orang-orang yang memasok dokumen. Operator harus memiliki kebijakan yang dipikirkan matang tentang bagaimana menangani permintaan atau permintaan dari lembaga penegak hukum (dari berbagai negara) untuk

y. Setelah Wikileaks merilis kabel yang dipilih, seluruh set dibuat publik di Web, baik secara tidak disengaja atau secara sengaja. Bagaimanapun, kegagalan untuk melindungi dokumen adalah kegagalan tanggung jawab.

tentang identitas seseorang yang memasok dokumen. Maksud dari beberapa kebocoran adalah untuk menyabot pesaing atau lawan politik. Verifikasi keaslian dan validitas dokumen yang bocor bisa sulit, tetapi ini merupakan tanggung jawab operator situs. Kerusakan serius bagi individu, bisnis, ekonomi, dan komunitas yang tidak bersalah dapat dihasilkan dari penerbitan dokumen yang tidak akurat atau dipalsukan dan kadang-kadang dari dokumen yang asli tetapi penuh dengan kebocoran.

Ketika sebuah surat kabar Jerman mengamati, "Ketika informasi yang rumit dipertaruhkan, kehati-hatian yang besar dituntut agar informasi tidak jatuh ke tangan yang salah dan agar orang tidak terluka." 38 Kebebasan berbicara dan pers meninggalkan kita dengan tanggung jawab etis untuk apa yang kami katakan dan publikasikan.

3.4 Anonimitas

Pers kolonial ditandai oleh penampilan yang tidak teratur, pseudonymous invective, dan kurangnya rasa hormat untuk segala bentuk pemerintahan.

- "Ilmu Pengetahuan, Teknologi, dan Amandemen Pertama," Kantor Teknologi AS

Menguji Sense Umum

Dari uraian yang dikutip di atas, pers Kolonial - pers penulis dari Amandemen Pertama Konstitusi AS menemukan itu sangat penting untuk dilindungi-memiliki banyak kesamaan dengan internet, termasuk kontroversi tentang anonimitas.

Jonathan Swift menerbitkan karangan politiknya, *Gulliver's Travels*, secara anonim. Nama Thomas Paine tidak muncul pada cetakan pertama *Common Sense*, buku yang membangkitkan dukungan untuk Revolusi Amerika. *The Federalist Papers*, diterbitkan di surat kabar pada 1787 dan 1788, berpendapat untuk mengadopsi Konstitusi AS yang baru. Para penulis, Alexander Hamilton, James Madison, dan John Jay, telah melayani konfederasi negara yang baru bebas dalam peran penting. Jay kemudian menjadi kepala mahkamah agung, Hamilton, sekretaris pertama Menteri Keuangan, dan presiden Madison. Tetapi ketika mereka menulis *the Federalist Papers*, mereka menggunakan nama samaran, Publius. Para penentang Konstitusi, mereka yang percaya itu memberi terlalu banyak kekuasaan kepada pemerintah federal, menggunakan nama samaran juga. Pada abad ke-19, ketika itu dianggap tidak pantas bagi perempuan untuk menulis buku, penulis seperti Mary Ann Evans dan Amantine Lucile Aurore Dupin diterbitkan dengan nama samaran laki-laki, atau nama pena (George Eliot dan George Sand). Orang-orang profesional dan akademis terkemuka menggunakan nama samaran untuk mempublikasikan misteri pembunuhan, fiksi ilmiah, atau karya non-akademis lainnya, dan beberapa penulis — misalnya, HL-ikon ikonoklastik — menggunakan nama samaran untuk kesenangannya.

Penggunaan anonimitas yang positif Keleluasaan

anonim bukanlah praktik yang merusak dan curang, tetapi sebuah tradisi advokasi dan perbedaan pendapat yang terhormat. Anonimitas adalah perisai dari tirani mayoritas.

—US Mahkamah Agung

Di Amerika Serikat, Amandemen Pertama melindungi pidato politik, tetapi masih ada banyak cara di mana pemerintah dapat membalas kritiknya. Ada juga banyak alasan pribadi mengapa seseorang mungkin tidak ingin dikenal untuk memiliki pandangan tertentu. Anonimitas memberikan perlindungan terhadap pembalasan dan rasa malu. Di Internet, orang berbicara tentang topik pribadi seperti kesehatan, kebiasaan berjudi, masalah dengan anak remaja, agama, dan sebagainya. Banyak orang menggunakan nama samaran ("pegangan," alias, atau nama layar) untuk menjaga identitas asli mereka tetap pribadi. Korban perkosaan dan jenis kekerasan dan pelecehan lainnya serta pengguna obat-obatan terlarang yang mencoba berhenti adalah di antara mereka yang mendapat manfaat dari sebuah forum di mana mereka dapat berbicara dengan jujur tanpa memberikan identitas mereka. (Dukungan pribadi dan kelompok konseling tradisional hanya menggunakan nama depan, untuk melindungi privasi.) Pelapor, melaporkan kegiatan yang tidak etis atau ilegal di tempat mereka bekerja, dapat memilih untuk melepaskan informasi secara anonim. Di masa perang dan di negara-negara dengan pemerintahan yang menindas, anonimitas bisa menjadi masalah hidup atau mati.

Bisnis menyediakan berbagai alat dan layanan canggih yang memungkinkan kami mengirim email dan menjelajahi Web secara anonim. Wartawan, aktivis hak asasi manusia, dan orang biasa menggunakan email anonim untuk melindungi diri mereka sendiri. Pendiri perusahaan yang menyediakan layanan anonim Web surfing mengatakan perusahaan mengembangkan alat untuk membantu orang-orang di Iran, China, dan Arab Saudi mendapatkan sekitar pembatasan pemerintah mereka pada akses Internet.⁴⁰ Banyak orang menggunakan browser Web anonim untuk menggagalkan upaya bisnis untuk mengumpulkan informasi tentang aktivitas Web mereka dan membuat dokumen untuk tujuan pemasaran.

Kita mungkin berpikir manfaat utama dari layanan anonimisasi adalah perlindungan bagi individu — melindungi privasi, melindungi terhadap pencurian identitas dan profil konsumen, dan melindungi terhadap pemerintah yang menindas. Namun, bisnis, lembaga penegak hukum, dan dinas intelijen pemerintah juga merupakan pelanggan utama. Sebuah bisnis mungkin ingin menyimpan penelitian dan perencanaannya tentang rahasia produk baru dari pesaing. Jika kompetitor dapat memperoleh log situs web yang dikunjungi oleh karyawan perusahaan, mereka mungkin dapat mencari tahu apa yang direncanakan perusahaan. Penyelaran Web Anonim membantu penyelidikan penegakan hukum. Misalkan agen penegak hukum mencurigai sebuah situs berisi pornografi anak, informasi teroris, materi yang melanggar hak cipta, atau hal lain yang relevan dengan investigasi. Jika mereka mengunjungi situs tersebut dari komputer departemen mereka, mereka mungkin diblokir atau melihat halaman hambar dengan tidak ada yang ilegal. Saya Juga, ketika agen penegak hukum pergi "bawah

y. situs web dapat menentukan alamat IP (yaitu urutan angka-angka yang mengidentifikasi domain atau komputer tertentu di Web) dari pengunjung dan dapat memblokir akses dari alamat tertentu atau memasang halaman alternatif untuk pengunjung tersebut.

Layanan remailer anonim

Johan Helsingius mendirikan layanan email anonim pertama yang terkenal di Finlandia pada tahun 1993. (Pengguna tidak sepenuhnya anonim; sistem tetap mengidentifikasi informasi.) Helsingius awalnya dimaksudkan layanannya untuk pengguna di Skandinavia negara-negara. Namun, layanan ini sangat populer dan tumbuh menjadi sekitar 500.000 pengguna di seluruh dunia. Helsingius menjadi pahlawan bagi para pembangkang di negara-negara totaliter dan untuk kebebasan berbicara dan privasi di mana-mana. Dia menutup layanannya pada tahun 1996 setelah Gereja Scientology dan pemerintah Singapura mengambil tindakan untuk mendapatkan nama-nama orang yang menggunakannya. Pada saat itu, banyak layanan serupa lainnya telah tersedia.

Untuk mengirim email anonim menggunakan layanan "ulang pengirim", seseorang mengirim pesan ke remailer, di mana alamat pengirim dihapus dan pesan dikirim kembali ke penerima yang dituju. Pesan dapat dirutekan melalui banyak tujuan antara hingga lebih sulit mengaburkan asal-usul mereka. Jika seseorang ingin tetap anonim tetapi menerima balasan, dia dapat menggunakan layanan di mana nomor ID berkode dilampirkan ke pesan ketika remailer mengirimkannya. ID yang diberikan oleh pengirim adalah samaran untuk pengirim, yang disimpan oleh remailer. Balasan masuk ke situs remailer, yang meneruskannya ke orang asli.

Beberapa layanan anonimitas menggunakan skema enkripsi untuk mencegah bahkan perusahaan yang mengoperasikannya dari mengidentifikasi pengguna.

cover "dan berpura-pura menjadi anggota atau calon korban dari kelompok kriminal online, mereka tidak ingin alamat IP mereka mengekspos mereka. Seorang pejabat senior CIA menjelaskan penggunaan layanan anonimitas CIA secara online: "Kami ingin beroperasi di mana saja di Internet dengan cara yang tidak seorang pun tahu CIA sedang melihat mereka."

41

Penggunaan anonimitas negative

Kami tidak dibebaskan dari etika biasa dan undang-undang hanya karena kita menggunakan Internet atau menandatangani komentar dengan alias daripada nama asli.

Anonimitas di dunia maya melindungi aktivitas kriminal dan antisosial. Orang menggunakannya untuk penipuan, pelecehan, dan pemerasan, untuk mendistribusikan pornografi anak, untuk mencemarkan nama baik atau mengancam orang lain dengan bebas hukuman, mencuri dokumen bisnis rahasia atau informasi kepemilikan lainnya, dan melanggar hak cipta. Postingan anonim dapat menyebarkan desas-desus palsu yang secara serius merusak bisnis, memanipulasi saham, atau menghasut kekerasan. Anonimitas membuat sulit untuk melacak pelaku kesalahan. Seperti enkripsi, teknologi anonimitas menimbulkan tantangan bagi penegak hukum.

Anonimitas dapat menyamarkan pengawasan ilegal oleh lembaga pemerintah — atau pengawasan legal namun reaktif di negara-negara yang tidak bebas. CIA membantu mendanai perusahaan rintisan anonim. Layanan anonimitas perusahaan memiliki kekurangan yang memungkinkan untuk menentukan identitas pengguna. Perusahaan telah mengumumkan bahwa CIA telah benar-benar meninjau produk, yang mengarah ke spekulasi bahwa CIA tahu tentang kekurangan dan senang memiliki perusahaan yang menawarkan layanan anonimisasi yang CIA bisa menghindari.⁴²

Apakah anonimitas dilindungi?

Bagi mereka yang tidak menggunakan layanan anonimitas sejati, kerahasiaan identitas kami di dunia maya tergantung baik pada kebijakan privasi penyedia layanan dan situs yang kami kunjungi — dan pada hukum dan putusan pengadilan tentang pemberian panggilan dari pengadilan untuk pengungkapan. Seberapa baik terlindungi identitas kita yang sebenarnya? Seberapa kuat mereka harus dilindungi?

Sebuah bisnis atau organisasi dapat memperoleh panggilan pengadilan yang memerintahkan ISP untuk mengungkapkan identitas asli seseorang. Dalam banyak kasus, bisnis mencari nama-nama orang yang memposting kritik, dilindungi oleh Amandemen Pertama, tetapi yang mungkin karyawan yang akan dipecat oleh bisnis tersebut. Pendukung pembicaraan bebas berpendapat bahwa hakim harus memeriksa kasus individu dan menentukan apakah bukti cukup kuat sehingga organisasi yang meminta identitas kemungkinan memenangkan gugatan — dan baru kemudian mengeluarkan panggilan pengadilan untuk nama asli seseorang. Beberapa merekomendasikan bahwa ISP diminta untuk memberi tahu anggota ketika ISP menerima panggilan pengadilan untuk identitas anggota, sehingga orang tersebut memiliki kesempatan untuk melawan somasi di pengadilan. Saran-saran ini dapat membantu melindungi kritik saat menahan orang yang bertanggung jawab atas pembicaraan ilegal.

Karena potensinya untuk melindungi aktivitas kriminal atau karena mereka menganggapnya tidak sesuai dengan kesopanan dan netiket (etika online), beberapa layanan dan komunitas online memilih untuk mencegah atau melarang anonimitas. Di sisi lain, situs web yang menyelenggarakan debat tentang isu kontroversial atau diskusi tentang topik yang sensitif secara sosial sering mempertanyakan anonimitas sebagai cara yang masuk akal untuk melindungi privasi dan mendorong diskusi yang terbuka dan jujur. Jika mereka yang bertanggung jawab atas layanan individual dan situs web membuat keputusan kebijakan tentang anonimitas, kebijakan dapat fleksibel dan beragam, disesuaikan dengan layanan dan klien tertentu.

Banyak masalah hukum tentang anonimitas mirip dengan yang ada dalam kontroversi penegakan hukum yang kita diskusikan di Bab 2. Lembaga penegak hukum telah mampu melacak banyak tersangka kriminal melalui Web (termasuk anggota kelompok peretas yang disebut Anonim). Haruskah tanggung jawab penegakan hukum untuk mengembangkan alat untuk menemukan penjahat yang bersembunyi di balik anonimitas, atau seharusnya tugas menjadi lebih mudah dengan mengharuskan kita mengidentifikasi diri kita sendiri? Apakah potensi bahaya oleh penjahat yang menggunakan anonimitas untuk bersembunyi dari penegak hukum lebih besar daripada hilangnya privasi dan menahan kebebasan berbicara bagi orang-orang jujur yang menggunakan anonimitas secara bertanggung jawab? Apakah anonimitas merupakan perlindungan penting terhadap kemungkinan penyalahgunaan kekuasaan pemerintah? Haruskah orang memiliki hak untuk menggunakan alat yang tersedia, termasuk anonymizers, untuk melindungi privasi mereka? Kami dapat mengirim email hardcopy tanpa alamat pengirim. Haruskah ada pembatasan lebih pada anonimitas di Internet daripada di konteks lain?

Sebuah contoh dari konservatisme dan arogansi yang tidak dapat dijelaskan dari otoritas bea cukai Turki baru-baru ini dibuktikan oleh larangan impor mesin ketik ke negara tersebut. Alasan yang dikemukakan oleh pihak berwenang untuk langkah ini adalah bahwa ketikan memberi ada tika-tika kepada penulis, dan oleh karena itu dalam hal durhaka atau menghina

pamflet atau tulisan dieksekusi oleh mesin tik yang beredar itu akan tidak mungkin untuk mendapatkan setiap keping mana operator mesin dapat dilacak. . . . Keputusan yang sama juga berlaku untuk stensil dan mesin duplikasi dan media sejenis lainnya. —Scientific American, 6 Juli 190143

3.5 Global Net: Sensor dan Kebebasan Politik

Rumah-rumah kopi muncul sebagai sumber utama berita dan desas-desus. Pada 1675, Charles II, curiga karena banyak penguasa adalah tempat di mana informasi perdagangan umum, menutup kedai kopi.

—Peter L. Bernstein⁴⁴

3.5.1 Alat untuk Komunikasi, Alat untuk Penindasan

Pemerintah otoriter telah mengambil langkah-langkah untuk memotong, atau secara serius mengurangi, aliran informasi dan opini sepanjang sejarah. Komunikasi yang semarak yang dimungkinkan oleh Internet mengancam pemerintah di negara-negara yang tidak memiliki kebebasan politik dan budaya. Untuk waktu yang lama, "kebijaksanaan konvensional" di antara pengguna dan pengamat Internet adalah bahwa itu adalah perlindungan terhadap penyensoran dan alat untuk meningkatkan kebebasan politik. Mesin email dan faks memainkan peran penting selama runtuhnya Uni Soviet dan demonstrasi demokrasi di Lapangan Tiananmen Cina. Situs web dengan konten yang ilegal di satu negara dapat disiapkan di beberapa negara lain. Orang-orang di negara-negara yang menyebutkan berita dapat mengakses informasi melalui Web dari tempat lain. Facebook dan ponsel adalah alat kunci dalam mengatur Musim Semi Arab 2011. Pembangunan di Iran, Vietnam, berbagai negara Timur Tengah, dan tempat lain menggunakan Skype untuk berkomunikasi karena enkripsi yang kuat. Ada banyak lagi contoh.

Sayangnya, tetapi tidak mengherankan, pemerintah yang opresif belajar dan mengadopsi tindakan balasan untuk memblokir arus informasi. Mereka menggunakan teknologi intersepsi dan pengawasan yang canggih untuk memata-matai warga mereka lebih teliti dari sebelumnya. Di bagian lain dari bagian ini, kami menggambarkan alat sensor dan intersepsi yang digunakan rezim opresif (dan beberapa demokrasi).

Di negara-negara seperti China dan Arab Saudi, di mana pemerintah nasional memiliki tulang punggung Internet (saluran komunikasi dan komputer tempat orang mengakses informasi), pemerintah memasang komputer mereka sendiri antara orang-orang mereka dan

^y Di Polandia, misalnya, sebelum pemerintah komunis jatuh pada tahun 1989, adalah ilegal untuk membuat fotokopi tanpa izin dari sensor pemerintah. Pemerintah lain telah melarang antena satelit dan telepon rumah.

3.5 Global Net: Sensor dan Kebebasan Politik 164 di

luar dunia. Mereka menggunakan firewall dan filter canggih untuk memblokir apa yang tidak ingin dilihat oleh orang-orangnya. Pemerintah Arab Saudi memblokir pornografi dan perjudian, seperti banyak negara mungkin, tetapi juga memblokir situs-situs pada keyakinan Bahai, Holocaust, dan konversi agama Muslim ke agama lain. Ini memblokir situs dengan informasi tentang anonymizers, alat untuk menggagalkan filter, dan enkripsi.

Turki melarang YouTube selama sekitar dua tahun. Pakistan melarang telepon Internet. Burma (Myanmar) melarang penggunaan Internet atau pembuatan halaman web tanpa izin resmi. Ini melarang posting materi tentang politik, serta posting dari setiap materi yang dianggap oleh pemerintah menjadi berbahaya bagi kebijakannya. (Di bawah undang-undang sebelumnya, kepemilikan modem atau antena satelit yang tidak sah dapat dikenai hukuman penjara hingga 15 tahun.) Banyak negara di Timur Tengah membatasi akses Internet. Vietnam menggunakan perangkat lunak penyaringan untuk menemukan dan memblokir pesan-pesan anti-komunis yang berasal dari negara lain.

Beberapa negara melarang Skype. Yang lain menumbangkannya. Sebelum revolusi di Mesir pada tahun 2011, pemerintah Mesir, misalnya, menggunakan spyware untuk mencegah komunikasi Skype. Mereka tidak merusak skema enkripsi Skype. Sebaliknya, tampaknya mereka menanam spyware di komputer orang yang mengganggu komunikasi sebelum dienkripsi di komputer pengirim atau setelah didekripsi di komputer penerima. Selama revolusi, pemerintah menutup sementara internet dan layanan telepon seluler sepenuhnya.

Pada 1990-an, ketika lebih sedikit orang menggunakan Web, pemerintah Cina mengharuskan pengguna Internet untuk mendaftar ke polisi. Di Cina dan negara-negara lain yang tidak maju, pemerintah berjuang dengan kesulitan memodernkan ekonomi dan teknologi mereka sambil mempertahankan kontrol ketat atas informasi. Sekarang, dengan ratusan juta pengguna Web, pemerintah secara ketat mengontrol dan menyensor apa yang dibaca orang dan apa yang mereka posting. Peraturan Cina melarang "menghasilkan, mengambil, menggandakan dan menyebarkan informasi yang dapat menghambat ketertiban umum." Situs dan topik yang dilarang atau disensor telah memasukkan Facebook, Google, New York Times, diskusi tentang demokrasi, situs keagamaan, organisasi hak asasi manusia, berita dan komentar tentang Taiwan dan Tibet, informasi tentang penyensoran (dan cara menghindarinya), berita ekonomi, dan laporan tentang kecelakaan besar atau bencana alam dan wabah penyakit. Pemerintah memblokir situs-situs Wikipedia berbahasa Mandarin dan Inggris selama sekitar satu tahun. Ribuan sensor memantau situs web. Ketika warga China mulai mengirim pesan untuk berkomunikasi tentang topik yang dilarang, pemerintah membentuk sistem untuk memfilter pesan tersebut.⁴⁵ Setelah protes etnis berubah menjadi kekerasan di satu wilayah, China memotong komunikasi, kemudian memblokir akses Internet di wilayah tersebut selama 10 bulan.

Pemerintah Iran, pada berbagai waktu, memblokir situs-situs amazon.com, Wikipedia, New York Times, dan YouTube. Ini juga memblokir situs yang menganjurkan akhir

y. Di mana teknologi belum tertangkap, pemerintah membatasi media komunikasi lama. Saingan presiden Zimbabwe Robert Mugabe dalam pemilihan presiden 2001 di Zimbabwe dituduh memiliki radio dua arah tanpa izin.

praktek merajam perempuan. Reporters Without Borders mengatakan bahwa Iran memblokir akses ke lebih dari lima juta situs web dalam beberapa tahun terakhir. Umumnya, pemerintah mengatakan blok situs untuk menjaga budaya Barat dekaden. Iran juga membuat siaran TV satelit. Pemerintah menggunakan alat pengawasan online yang canggih dan melatih polisi cyber untuk memata-matai para pembangkang. Sistem mereka memeriksa paket-paket individual dari email, percakapan telepon, gambar, komunikasi jejaring sosial, dan seterusnya. Di beberapa negara, agen pemerintah, menggunakan media sosial, berpura-pura menjadi pembangkang dan menyebarkan informasi tentang protes yang direncanakan; polisi menangkap siapa saja yang datang. Beberapa pemerintah (misalnya, Tunisia dan Libya sebelum revolusi tahun 2011) menghentikan komunikasi dan menggunakan spyware di situs-situs seperti Facebook dan Yahoo untuk mengumpulkan kata sandi, menemukan nama-nama blogger pembangkang, dan menghapus halaman yang kritis terhadap pemerintah. Beberapa pemerintah (misalnya, Cina, Iran, Rusia, Vietnam) melarang atau melarang layanan email dan situs jejaring sosial yang berbasis di Barat dan mendirikan situs mereka sendiri — yang tentu saja mereka kendalikan.⁴⁶ Seperti yang akan kita lihat dalam Bagian 3.5.2, pemerintah yang membatasi semakin menggunakan leverage mereka atas perusahaan yang ingin melakukan bisnis di negara mereka untuk menegakkan persyaratan sensor dan standar konten lainnya. Akankah internet dan teknologi komunikasi terkait menjadi alat untuk meningkatkan kebebasan politik, atau akankah mereka memberikan kekuatan lebih kepada pemerintah untuk memata-matai, mengendalikan, dan membatasi orang-orang mereka?

Kantor komunikasi diperintahkan untuk menemukan cara untuk memastikan bahwa penggunaan Internet menjadi tidak mungkin. Kementerian untuk Promosi Kebajikan dan Pencegahan Wakil wajib memantau perintah dan menghukum pelanggar.

- Kutipan dari dekrit Taliban yang melarang semua penggunaan Internet di Afghanistan, 2001⁴⁷

3.5.2 Membantu Sensor Asing dan Rejim represif

Kebebasan berekspresi bukanlah prinsip kecil yang dapat disingkirkan ketika berurusan dengan kediktatoran.

—Reporters Without Borders⁴⁸

Menyediakan layanan, mematuhi hukum setempat

Perusahaan mesin pencari, perusahaan media sosial, dan perusahaan berita dan hiburan yang berbasis di negara-negara bebas menawarkan layanan di negara-negara dengan sensor ketat dan pemerintah yang represif. Untuk beroperasi dalam suatu negara, perusahaan harus mengikuti undang-undang negara tersebut. Apa trade-off antara menyediakan layanan kepada orang-orang dan mematuhi persyaratan sensor pemerintah? Sejauh mana, atau seharusnya, prospek

dari peluang bisnis besar di negara baru mempengaruhi keputusan perusahaan? Bagaimana perusahaan menangani persyaratan penyensoran? Apa tanggung jawab etis mereka? Situs-situs Cina dari Yahoo dan MSN mematuhi hukum setempat dan menghilangkan berita yang menyinggung pemerintah. Microsoft mengatakan itu menyensor istilah seperti "kebebasan" dan "demokrasi" di portal Cina-nya. Microsoft juga menutup blog jurnalis China di situs MSN Spaces yang mengkritik pemerintah China.⁴⁹ Yahoo memberikan informasi kepada pemerintah China yang membantu mengidentifikasi setidaknya dua orang yang kemudian dipenjarakan karena penulisan pro-demokrasi. Yahoo mengatakan bahwa mereka harus mematuhi hukum Tiongkok dan perusahaan belum diberitahu alasan permintaan pemerintah atas informasi tersebut. Untuk beroperasi di China, pemerintah China mengharuskan Skype untuk bekerja dalam usaha patungan dengan perusahaan komunikasi China (TOM), menggunakan versi modifikasi dari perangkat lunak Skype, dan menyaring topik sensitif dari obrolan teks. Menurut sebuah penelitian oleh universitas Kanada, perangkat lunak yang dimodifikasi memungkinkan pengawasan luas, dan TOM menyimpan informasi dari jutaan pesan.

Google telah lama mempromosikan ideal akses ke informasi. Google bertahan lebih lama daripada beberapa perusahaan, menolak untuk menyensor mesin pencariannya, meskipun telah mengambil beberapa langkah untuk membatasi akses ke informasi di China. Pada 2006, Google mengecewakan banyak pembicara kebebasan berbicara dan hak asasi manusia dengan memperkenalkan versi China di China, google.cn, yang akan sesuai dengan hukum China. Hasil pencariannya tidak menunjukkan situs dengan konten yang dilarang. Google menyimpulkan bahwa perusahaan tidak dapat menyediakan layanan tingkat tinggi di China tanpa kehadiran lokal. Dengan demikian, perjanjian untuk beroperasi di China dan memblokir material yang dianggap pemerintah sensitif adalah keputusan bahwa beberapa akses lebih baik daripada tidak ada akses. Google co-founder Sergey Brin, yang lahir di Uni Soviet dan mengalami pemerintahan totaliter, merasa tidak nyaman dengan keputusan sensor 2006. Google menghentikan pengoperasian mesin pencari yang disensor pada tahun 2010. Perusahaan menarik sebagian besar operasi dari China tetapi menawarkan layanan pencariannya melalui Hong Kong, yang meskipun sebagian dari Tiongkok, memiliki undang-undang yang berbeda. Dorongan utama untuk perubahan adalah serangan hack yang sangat canggih yang berasal dari China di Google dan sekitar 30 perusahaan lainnya. Tujuan utama serangan itu tampaknya adalah akses ke akun Gmail para aktivis hak asasi manusia China, yang membuat marah Brin dan yang lainnya di Google. Penolakan awal Google untuk menyensor, pembalikan pada tahun 2006, dan pembalikannya lagi pada tahun 2010 menggambarkan kesulitan memutuskan bagaimana menangani pemerintah yang represif. Kemudian, Google meningkatkan operasi di China yang tidak disensor, seperti pencarian produk dan sistem operasi Android.

Ketika AS atau perusahaan non-Cina lainnya mendirikan cabang di China dan mematuhi undang-undang yang membatasi, haruskah kita melihatnya sebagai menyediakan lebih banyak akses ke informasi di China daripada yang ada, meskipun tidak sebanyak mungkin secara teknis? Haruskah kita melihat mereka menghormati budaya dan hukum negara tuan rumah dengan tepat? Haruskah kita memandang mereka sebagai mitra dalam pembatasan etis yang tidak dapat diterima oleh pemerintah Cina dalam debat dan akses ke informasi oleh warganya?

Mark Zuckerberg, CEO Facebook, menyarankan bahwa keuntungan dari jejaring sosial di Tiongkok lebih besar daripada batasannya. Kita dapat melihat argumen ini, mirip dengan

argumen dari perusahaan lain untuk mematuhi tuntutan pemerintah otoriter, sebagai argumen utilitarian. Jika sebuah perusahaan menyerahkan nama-nama orang yang melanggar hukum penyensoran, pemerintah menangkap sejumlah kecil pembangkang, tetapi sejumlah besar orang mendapat manfaat dari peningkatan layanan dan komunikasi. Namun, jika kita mempertimbangkan efek jangka panjang, kita harus mempertimbangkan bahwa kerja sejumlah kecil orang yang tidak setuju dapat berdampak besar pada kebebasan masyarakat secara keseluruhan. Seseorang dapat membuat argumen utilitarian lainnya (kuat dan lemah). Penangkapan seorang pembangkang mungkin memicu protes yang akhirnya membawa lebih banyak kebebasan — atau tindakan keras yang brutal. Sistem etika berbasis hak dapat menerima penyediaan layanan pencarian atau media sosial yang agak terbatas. Orang-orang memiliki hak (etis, meskipun tidak sah) untuk mencari dan berbagi informasi, tetapi penyedia layanan tidak berkewajiban secara etis untuk memberikannya 100%. Namun, pandangan berbasis hak mengatakan kepada kita adalah salah untuk membantu memenjarakan seseorang karena mengekspresikan pandangannya tentang politik atau mengkritik pemerintah. Haruskah perusahaan menarik garis, mungkin setuju untuk membatasi akses informasi tetapi menolak untuk mengungkapkan informasi yang dapat digunakan pemerintah untuk memenjarakan seseorang karena menerbitkan pandangannya? Pemerintah mungkin perlu mengidentifikasi seseorang yang dicurigai menguntit, penipuan, memposting pornografi anak, atau kejahatan lainnya. Seorang penyedia layanan mungkin ingin memberikan informasi dalam kasus-kasus kriminal semacam itu. Jika pemerintah tidak mengungkapkan alasan permintaan, atau tidak jujur tentang alasannya, bagaimana penyedia layanan dapat membuat keputusan etis?

Kami mengizinkan terlalu banyak, mungkin, kebebasan berbicara di negara-negara yang belum mengalaminya sebelumnya.

—Adam Conner, seorang pelobi Facebook⁵⁰

Jangan jahat.

—Motto perusahaan informal Google

Menjual alat-alat pengintaian

Mungkin tidak mengherankan jika pemerintah yang represif mencegat komunikasi dan menyaring konten Internet. Sangat mengganggu bahwa perusahaan-perusahaan di negara-negara demokrasi Barat (termasuk Inggris, Jerman, Perancis, dan Amerika Serikat) menjual alat-alat itu kepada mereka. Perusahaan menjual alat canggih kepada pemerintah untuk menyaring konten Internet, meretas ponsel dan komputer, memblokir pesan teks, mengumpulkan dan menganalisis sejumlah besar data Internet, menanam spyware dan malware lainnya (perangkat lunak berbahaya), memantau jaringan sosial, dan melacak pengguna ponsel. Perusahaan-perusahaan mengatakan alat-alat itu untuk investigasi kriminal (serta mendeteksi dan menyaring konten yang tidak diinginkan) dan tidak melanggar hukum negara yang menggunakannya. Tentu saja, negara-negara dengan pemerintahan yang represif memiliki penjahat dan teroris juga. Apakah kita mempercayai pemerintah-pemerintah ini untuk menggunakan perangkat hanya terhadap orang-orang jahat, dengan cara yang konsisten dengan hak asasi manusia? Apakah etis bagi perusahaan di negara-negara bebas untuk menjual alat-alat kepada pemerintahan yang represif?

Kita tidak benar-benar bertanya, "Apakah ini demi kepentingan publik?"

—Penyelenggara pameran dagang untuk perusahaan yang menjual peralatan peretasan dan intersepsi kepada pemerintah⁵¹

3.5.3 Mematikan Komunikasi di Negara-negara Bebas

Pemerintah di negara-negara yang relatif tidak bebas yang secara ketat mengendalikan komunikasi menutup akses ke Internet atau mematikan layanan ponsel sesekali. Kejadian-kejadian ini membangkitkan kritik di dunia bebas, di mana sedikit yang diharapkan bisa terjadi. Kemudian pemerintah Inggris dan beberapa kota di AS menganggapnya, dan sistem transit di San Francisco memblokir layanan telepon seluler selama beberapa jam, mengangkat isu-isu baru untuk komunikasi di negara-negara bebas. Memberi wewenang pemerintah untuk menutup komunikasi menimbulkan ancaman nyata terhadap kebebasan berbicara, kegiatan biasa, dan kebebasan politik. Apakah masuk akal dalam situasi terbatas ketika keselamatan publik terancam? Apakah menutup layanan komunikasi di negara-negara bebas memberikan alasan kepada para diktator? Bisakah kita membuat perbedaan yang jelas antara tanggapan jangka pendek terhadap massa yang penuh kekerasan di negara-negara bebas dan penyensoran dan penindasan terhadap diskusi politik di negara-negara yang tidak bebas? Sebagai latar belakang untuk memikirkan pertanyaan-pertanyaan ini, kami mempertimbangkan insiden di Inggris dan Amerika Serikat.

Gerombolan hooligan (kata kuno itu tampaknya cocok) mengamuk di lingkungan tetangga di London dan kota-kota Inggris lainnya yang membakar, merampok bisnis, dan memukuli orang-orang yang mencoba melindungi diri atau harta mereka. Mereka merencanakan dan mengoordinasikan serangan mereka menggunakan ponsel, Twitter, BlackBerry Messenger, dan alat-alat serupa. Selama kekerasan, orang-orang di pemerintahan (dan lainnya) berpendapat bahwa Research In Missions harus mematikan BlackBerry Messenger. (Tidak.) Setelah kerusuhan, pemerintah Inggris mempertimbangkan untuk mencari perundang-undangan yang mengijinkannya untuk menutup sistem komunikasi seperti media sosial dan sistem pesan dalam situasi seperti itu. Sudah diputuskan, setidaknya untuk saat ini, untuk tidak mencari kekuatan semacam itu. Beberapa kota AS yang mengalami kekerasan terkoordinasi bilateral dianggap hukum untuk mengotorisasi lembaga pemerintah untuk memblokir komunikasi, tetapi tidak ada yang meloloskan undang-undang tersebut.

Tak lama setelah kekerasan di Inggris, sistem Bay Area Rapid Transit (BART) di San Francisco Bay Area mematikan layanan nirkabel di beberapa stasiun kereta bawah tanah setelah mengetahui rencana untuk "menggunakan perangkat seluler untuk berkoordinasi. . . kegiatan yang mengganggu dan berkomunikasi tentang lokasi dan jumlah Polisi BART." ⁵² BART memiliki peralatan komunikasi; Dikatakan kontraknya dengan perusahaan layanan seluler memungkinkannya mematikan layanan ketika dianggap perlu. Para manajer bisnis swasta, mengharapkan kekerasan di atau dekat properti mereka, memiliki hak untuk mematikan layanan nirkabel mereka; menolak masuk ke siapa pun yang membawa, katakanlah, tongkat baseball; atau tutup jika mereka menganggapnya sebagai tindakan bijaksana untuk melindungi publik dan bisnis. Jika BART adalah perusahaan swasta, akan ada argumen di kedua sisi pertanyaan apakah tindakannya bijaksana, tetapi tidak akan meningkatkan masalah Amandemen Pertama dari shutdown yang diperintahkan oleh pemerintah. (Beberapa argumen, dan perbedaan antara pemerintah dan tindakan swasta, mirip dengan yang berkaitan dengan hak layanan komputer untuk menyaring spam; lihat Bagian 3.2.4.)

BART adalah lembaga pemerintah, tetapi ia mematikan layanan nirkabel sendiri di ruangnya sendiri. Apakah itu mengancam kebebasan berbicara, atau apakah itu keputusan keamanan yang sah?

Apa yang bisa dilakukan, pendeknya komunikasi mematikan, untuk mengurangi penggunaan sistem semacam itu untuk merencanakan kekerasan massal? Kebijakan keanggotaan dari berbagai perusahaan media sosial melarang ancaman kekerasan. Facebook, misalnya, memantau posting untuk menegakkan larangannya. Perusahaan-perusahaan dapat menutup akun-akun mereka yang melanggar perjanjian, tetapi tidak mungkin perusahaan-perusahaan tersebut akan dapat bertindak cukup cepat untuk menghentikan peristiwa kekerasan. Dalam kerusuhan masa lalu, polisi mengumpulkan informasi dari media sosial dan telepon orang-orang yang mereka tangkap, dan dengan demikian mereka mengetahui rencana untuk serangan yang lebih keras dan siap untuk mencegahnya. Meskipun bermanfaat, ini juga tampak seperti perlindungan yang lemah. Tapi apa konsekuensi memberi pemerintah wewenang untuk menutup komunikasi? Polisi dapat menyalahgunakan kekuasaan ini, mencegah protes dan demonstrasi yang sah, seperti yang dilakukan oleh pemerintah yang represif. Penghentian skala besar akan menyebabkan ketidaknyamanan (dan mungkin membahayakan) orang yang tidak bersalah. Di Amerika Serikat, Mahkamah Agung mungkin akan menyatakan tidak konstitusionalnya sebuah undang-undang yang memberi wewenang kepada lembaga pemerintah untuk memerintahkan layanan komunikasi pribadi untuk ditutup. Apa lagi yang bisa dilakukan?

Ini mungkin peralatan BART, tetapi itu tidak berarti bahwa mereka memiliki kebebasan untuk melakukan apa pun yang mereka inginkan dengan itu. —Michael Risher, pengacara ACLU 53

3.6 Regulasi Netralitas Bersih atau Pasar?

Penyensoran langsung bukan satu-satunya faktor yang dapat membatasi jumlah dan variasi informasi yang tersedia bagi kita di Internet. Struktur peraturan mempengaruhi ketersediaan layanan dan tingkat inovasi. Perusahaan besar sering melobi undang-undang dan peraturan untuk membatasi persaingan: Jaringan televisi AS menunda kabel selama lebih dari satu dekade. Selama beberapa dekade, perusahaan penyiaran melobi untuk menjaga stasiun radio berdaya rendah (disebut "radio mikro") hampir ilegal. "Netralitas bersih" mengacu pada berbagai proposal untuk pembatasan tentang bagaimana perusahaan telepon dan kabel berinteraksi dengan pelanggan broadband mereka (terutama untuk layanan Internet) dan bagaimana mereka menetapkan biaya untuk layanan. Ada dua masalah yang berbeda tetapi terkait, kadang-kadang kabur dalam argumen: (1) apakah perusahaan yang menyediakan jaringan komunikasi harus diizinkan untuk mengecualikan atau memberikan perlakuan berbeda terhadap konten berdasarkan konten itu sendiri, pada kategori konten, atau pada perusahaan atau organisasi yang menyediakannya, dan (2) apakah perusahaan yang menyediakan jaringan komunikasi harus diizinkan untuk menawarkan penyedia konten dan pelanggan individu dengan tingkat kecepatan dan prioritas yang berbeda pada tingkat harga yang berbeda. Yang terakhir ini kadang disebut layanan "berjenjang" —yaitu, tingkat layanan berbeda dengan biaya yang berbeda. Perusahaan yang sangat besar berada di kedua sisi perdebatan, seperti organisasi dan orang-orang terkemuka yang ingin mempertahankan keterbukaan dan vitalitas dari Net.

Advokat "netralitas bersih" ingin pemerintah memberi mandat bahwa perusahaan telekomunikasi memperlakukan semua konten hukum yang bergerak melalui jalur broadband dan jaringan nirkabel mereka dengan cara yang sama. Perlakuan yang sama mencakup pengisian semua pelanggan dengan tarif yang sama untuk mengirim informasi melalui Internet dan tidak mengutamakan konten atau pelanggan tertentu. Netralitas akan mengembalikan sebagian dari konsep pembawa umum (seperti yang dijelaskan dalam Bagian 3.1), sebagian didasarkan pada pandangan bahwa perusahaan telepon (sekarang telepon dan kabel) memiliki monopoli transmisi informasi dan bahwa perusahaan yang mengontrol transmisi tidak boleh diizinkan untuk mengontrol akses ke konten juga. Banyak penyedia konten Internet, termasuk blogger individu dan perusahaan besar seperti eBay, Microsoft, Amazon, Netflix, dan Google, berdebat untuk aturan netralitas-net. Tanpa aturan, ada yang berpendapat, mereka harus membayar tarif lebih tinggi dan perusahaan komunikasi akan memberikan perlakuan khusus kepada penyedia konten mereka sendiri. Beberapa kelompok berpendapat bahwa memungkinkan perusahaan komunikasi untuk menetapkan tingkat yang berbeda akan sangat merusak Internet karena akan memeras suara independen.

Pengisian tarif yang berbeda untuk produk dan layanan tidak biasa dan masuk akal secara ekonomi di banyak area. Jurnal penelitian membebani perpustakaan dengan tingkat berlangganan lebih tinggi daripada biaya individu, karena lebih banyak orang membaca setiap salinan pustaka. Banyak bisnis memberikan diskon dalam jumlah besar. Beberapa lembaga dan bisnis — rumah sakit, misalnya — membayar tarif yang lebih tinggi untuk layanan seperti listrik di bawah kontrak yang menjamin prioritas lebih tinggi untuk perbaikan atau layanan darurat bila diperlukan. Kita semua memiliki pilihan membayar biaya pengiriman standar untuk produk yang kita beli secara online atau membayar lebih untuk pengiriman lebih cepat. Orang membayar untuk berkendaraan di jalur ekspres di jalan raya; harga mungkin berbeda dengan waktu hari dan tingkat lalu lintas. Dengan demikian, gagasan bahwa setiap pelanggan harus membayar jumlah yang sama tidak memiliki manfaat intrinsik. Apakah ada manfaat untuk internet? Apakah masuk akal bagi operator komunikasi untuk, katakanlah, kontrak dengan pemasok video untuk menyediakan pengiriman video lebih cepat dengan biaya tertentu?

Pendukung harga netral takut bahwa kurangnya pengaturan harga akan mengikis keragaman Internet. Hanya perusahaan dan organisasi besar yang mampu membayar harga yang diperlukan untuk memastikan bahwa konten mereka bergerak cukup cepat agar relevan. Konten yang diberikan individu dan organisasi yang lebih kecil akan hilang. Beberapa berpendapat bahwa harga fleksibel akan memberikan perusahaan telekomunikasi terlalu banyak kekuasaan atas konten di Internet. Pendukung netralitas bersih melihat layanan berjenjang sebagai ancaman terhadap inovasi, partisipasi demokratis, dan kebebasan berbicara online. Vinton Cerf, Wakil Presiden dan Kepala Penginjil Internet di Google dan pelopor internet yang sangat dihormati, melihat netralitas operator, kurangnya penjaminan dan kontrol terpusat, sebagai faktor kunci yang bertanggung jawab atas keberhasilan Net dan inovasi seperti blogging dan telepon Internet. Dia berpendapat bahwa tidak ada cukup kompetisi di industri operator jaringan untuk melindungi terhadap pelanggaran.⁵⁴

y Sungguh, itulah gelarnya.

Para penentang netralitas bersih berpendapat bahwa peraturan netralitas akan memperlambat kemajuan koneksi Internet berkecepatan tinggi dan perbaikan infrastruktur. Sebelum FCC melonggarkan peraturan lama (pada tahun 2003–2005), perusahaan telekomunikasi hanya memiliki sedikit insentif untuk berinvestasi dalam kapasitas broadband. Dalam beberapa tahun sesudahnya, mereka menginvestasikan ratusan miliar dolar. Kecepatan meningkat, harga turun, dan kapasitas tambahan sangat penting untuk fenomena baru seperti streaming film. Investasi berkelanjutan dalam broadband diperlukan untuk pertumbuhan di berbagai bidang seperti layanan backup online, semua data yang kami terima di ponsel, aplikasi sensor jarak jauh, inovasi dalam layanan pendidikan, dan sebagainya. Para penentang peraturan tambahan mengatakan tidak boleh ada peraturan baru yang besar tanpa bukti bahaya dalam sistem saat ini. David Farber, perintis Internet lain yang sangat dihormati, menentang undang-undang netralitas: "Kami tidak ingin secara tidak sengaja menghentikan inovasi dengan menerapkan aturan atau undang-undang yang implikasinya jauh dari jelas." 55 Beberapa yang mendukung pasar bebas menentang mandat harga seragam pada prinsip , sebagai gangguan yang tidak etis dalam pilihan bebas penjual dan pembeli.

Peningkatan besar dalam lalu lintas karena smartphone dan tablet meningkatkan netralitas bersih. Pada 2010, video menghasilkan lebih dari 75% lalu lintas data seluler. Apakah masuk akal untuk memperlakukan lalu lintas semacam itu secara berbeda? Haruskah itu memiliki prioritas tinggi (seperti panggilan suara) karena penundaan mengganggu pelanggan? Haruskah itu memiliki prioritas lebih rendah karena menggunakan begitu banyak bandwidth? Haruskah penyedia layanan membuat keputusan ini, atau haruskah Kongres dan FCC membuatnya? Ketika orang menonton video di smartphone, mereka sering tidak menonton semuanya. Sebuah perusahaan mengembangkan teknik untuk mengirim video ke pengguna dalam segmen saat dia menonton (tanpa penundaan yang meningkat), daripada mengirim seluruh video secepat mungkin. Perusahaan mengatakan pendekatan ini dapat memotong transfer data menjadi setengahnya. Dapatkah regulator menulis aturan netralitas bersih yang memungkinkan atau mendorong solusi teknologi seperti itu untuk mengurangi lalu lintas, atau aturan kaku akan menghambat atau menghambatnya?

Status hukum netralitas bersih masih belum jelas. Ketika Comcast memperlambat beberapa lalu lintas dari situs tertentu pada tahun 2007, FCC mengatakan bahwa perusahaan melanggar pedoman FCC dan memerintahkannya untuk berhenti. Pengadilan federal memutuskan bahwa FCC tidak memiliki otoritas hukum untuk melakukannya. Kongres belum memberi otoritas FCC untuk membuat aturan untuk Internet. FCC mengeluarkan aturan, bagaimanapun, pada tahun 2011; tantangan pengadilan sedang berlangsung.

Tinjau Latihan

- 3.1 Jelaskan secara singkat perbedaan antara operator umum, penyiar, dan penerbit sehubungan dengan kebebasan berbicara dan kontrol konten.
- 3.2 Jelaskan dua metode yang dapat digunakan orang tua untuk membatasi akses oleh anak-anak mereka ke materi yang tidak pantas di Web.
- 3.3 Apa salah satu alasan utama mengapa pengadilan memutuskan ketentuan penyensoran Undang-Undang Ketepatan Anggaran yang melanggar Amandemen Pertama?
- 3.4 Apa salah satu cara untuk mengurangi spam?
- 3.5 Dokumen apa yang dibuat WikiLeaks untuk umum?
- 3.6 Berikan contoh publikasi anonim lebih dari 100 tahun yang lalu.
- 3.7 Menyebutkan dua metode yang digunakan beberapa pemerintah untuk mengendalikan akses ke informasi.

Latihan Umum

- 3.8 Sebuah perusahaan besar memiliki kebijakan yang melarang karyawan menulis blog tentang produk perusahaan. Apa sajakah alasan yang mungkin untuk kebijakan tersebut? Apakah itu melanggar Amandemen Pertama? Apakah ini masuk akal?
- 3.9 Bagaimana Internet mengubah pengertian standar komunitas untuk menentukan apakah materi secara hukum tidak senonoh? Menurut Anda, kriteria standar komunitas dapat dipertahankan di Internet? Jika ya, jelaskan caranya. Jika tidak, jelaskan alasannya.
- 3.10 Kebijakan apa untuk akses Internet dan penggunaan perangkat lunak penyaring menurut Anda sesuai untuk dasar sekolah? Untuk sekolah menengah? Berikan alasan Anda.
- 3.11 Berbagai organisasi dan anggota Kongres menyarankan untuk mensyaratkan situs Web yang mengandung materi “berbahaya bagi anak di bawah umur” untuk pindah ke domain Web baru “.xxx”. Berikan beberapa alasan untuk dan menentang persyaratan semacam itu.
- 3.12 RUU diperkenalkan di Kongres untuk mewajibkan situs web dengan pornografi mendapatkan bukti usia dari siapa saja yang mencoba mengunjungi situs, mungkin dengan meminta nomor kartu kredit atau nomor identifikasi orang dewasa lainnya. Diskusikan beberapa argumen untuk dan melawan hukum semacam itu.
- 3.13 Anggota staf perpustakaan di dua kota mengajukan keluhan kepada Komisi Kesempatan Kerja Persamaan federal (EEOC) dengan alasan bahwa mereka dikenai "lingkungan kerja yang tidak ramah." Perpustakaan tempat mereka bekerja tidak menyediakan filter di terminal Internet. Para staf dipaksa untuk melihat materi yang menyinggung pada layar pengguna perpustakaan dan cetakan pornografi yang ditinggalkan di printer perpustakaan. Diskusikan konflik antara lingkungan kerja yang bermusuhan dan kebebasan berbicara dalam situasi ini. Tanpa mempertimbangkan undang-undang saat ini, bagaimana Anda menyelesaikan konflik di sini?
- 3.14 Empat siswa sekolah menengah menemukan instruksi untuk membuat bom di situs web. Mereka membangun bom dan memasangnya di lorong sekolah mereka. Salah satu siswa, berusia 18 tahun, mengatakan mereka tidak tahu seberapa kuat bom itu dan mereka tidak punya niat menyakiti siapa pun. Dia berkomentar, “Ini adalah situs yang sangat berbahaya. . . . Saya bukan pembuat onar atau apa pun. Saya hanya anak biasa.”⁵⁶ Evaluasilah komentarnya.
- 3.15 Misalkan Anda menulis hukum antispam. Menurut Anda, apa definisi spam yang masuk akal dalam konteks ini? Tunjukkan jumlah pesan dan bagaimana hukum akan menentukan apakah pesan itu tidak diminta.
- 3.16 Peraturan dan undang-undang federal di beberapa negara bagian (beberapa lama, beberapa disahkan khusus untuk Internet) melarang atau membatasi banyak jenis penjualan online. Misalnya, undang-undang membatasi penjualan lensa kontak, peti mati, dan obat resep di Web. Undang-undang melarang produsen mobil menjual mobil langsung kepada konsumen di Internet. Lembaga Kebijakan Progresif memperkirakan bahwa undang-undang negara bagian seperti itu membebani konsumen setidaknya \$ 15 miliar per tahun.⁵⁷
- Di antara undang-undang ini mana yang dapat Anda pikirkan alasan yang baik? Mana yang lebih mirip dengan undang-undang anti-persaingan yang dijelaskan dalam Bagian 3.2.5?

y Item spesifik yang penjualan atau pembeliannya secara online dilarang atau dibatasi mungkin telah berubah.

- 3.17 Dalam Bagian 3.3, kami melihat bahwa orang-orang mengkritik Yahoo karena memperluas toko onlinenya untuk materi dewasa, dan orang-orang mengkritik Yahoo karena menanggapi keluhan, membatalkan kebijakan baru, dan menghapus iklan untuk materi dewasa. Apa pendapat Anda tentang keputusan Yahoo? Apa pendapat Anda tentang kedua kritik itu?
- 3.18 Sebuah situs web yang menerbitkan dokumen yang bocor memposting konten akun email Yahoo dari calon presiden selama kampanye pemilihan.
- (a) Jelaskan beberapa jenis hal yang mungkin ada di antara dokumen-dokumen yang bocor yang akan berharga bagi lawan-lawan calon.
- (b) Jelaskan beberapa hal yang mungkin ada di antara dokumen yang bocor yang dapat merugikan kampanye tetapi tidak menunjukkan kesalahan apa pun.
- (c) Buatlah standar etika untuk memposting konten dari akun yang Anda akan merasa nyaman dengan tidak peduli apakah Anda mendukung atau menentang kandidat.
- 3.19 Anda mengetahui sebuah penelitian yang menyimpulkan bahwa sistem darurat California, termasuk rumah sakit, persediaan darurat, polisi, dan sebagainya, tidak cukup untuk menanggapi besarnya kemungkinan gempa yang akan terjadi dalam 30 tahun ke depan. Studi ini belum dirilis ke publik, dan Anda berpikir untuk membocorkannya ke situs web yang menerbitkan dokumen yang bocor. Buat daftar manfaat dari membocorkan penelitian dan risiko melakukannya. Buat daftar pertanyaan lain yang Anda anggap relevan untuk membuat keputusan. Tunjukkan bagaimana jawaban yang berbeda untuk beberapa pertanyaan dapat memengaruhi keputusan Anda.
- 3.20 Astronom amatir di seluruh dunia telah menemukan dan melacak satelit - baik satelit komersial dan mata-mata - dan memposting orbitnya di Web.58 Beberapa pejabat intelijen berpendapat bahwa jika musuh dan teroris tahu ketika satelit mata-mata AS berada di atas, mereka dapat menyembunyikan kegiatan mereka. Masalah apa yang ditimbulkan masalah ini? Haruskah para astronom menahan diri dari memposting orbit satelit? Mengapa atau mengapa tidak?
- 3.21 Seseorang memposting video di situs video populer yang menunjukkan sekelompok pria dengan klub memasuki gedung dan memukul orang yang tidak bersenjata. Kebijakan situs melarang memposting video dengan kekerasan grafis. Ketika seorang pemirsa mengeluh, situs tersebut menghapus video tersebut. Pemirsa lain mengajukan banding atas penghapusan tersebut, dengan mengatakan video tersebut mendokumentasikan penyalahgunaan tahanan di kamp penjara Rusia. Misalkan Anda seorang manajer di situs tersebut. Kembangkan rencana untuk menangani video semacam itu. Maukah Anda mem-posting ulang videonya? Jelaskan masalah yang Anda pertimbangkan.
- 3.22 Sebuah situs web anti-aborsi mempublikasikan daftar dokter yang melakukan aborsi dan hakim serta politisi yang mendukung hak aborsi. Ini termasuk alamat dan informasi pribadi lainnya tentang beberapa orang. Ketika para dokter dalam daftar itu terluka atau terbunuh, situs itu melaporkan hasilnya. Gugatan untuk menutup situs karena menghasut kekerasan gagal. Keputusan pengadilan banding yang kontroversial menemukan itu menjadi latihan legal kebebasan berbicara. Masalah penting adalah garis tipis antara ancaman dan pidato yang dilindungi, masalah sulit yang mendahului Internet. Apakah fakta bahwa ini adalah situs web daripada newsletter dicetak dan dikirimkan membuat perbedaan? Apa, jika ada, masalah dalam hal ini terkait dengan dampak Internet?
- 3.23 Uni Eropa memiliki undang-undang yang membatasi persentase pemrograman media audio-visual (awalnya terutama televisi, tetapi sekarang termasuk konten Internet) yang diproduksi di luar UE. Kanada memiliki pembatasan serupa pada konten radio dan televisi. Orang-orang di industri film Kanada telah mengajukan kuota pada film asing. Alasan yang diberikan termasuk melindungi budaya suatu negara dan

melindungi perusahaan konten mereka dari persaingan asing.

(a) Apakah menurut Anda pembatasan tersebut masuk akal? Apakah Anda pikir mereka akan tetap efektif dengan perluasan media online dalam beberapa tahun terakhir? Alasan memberi.

(b) Amerika Serikat tidak memiliki kuota semacam itu pada program atau film asing. Anda, Menurut mengapa ini terjadi?

- 3.24 Adalah ilegal bagi kelompok-kelompok amal bebas pajak untuk melakukan lobi politik. Situs web dari banyak organisasi semacam itu memiliki tautan ke situs organisasi yang melakukan lobi. Sebagai contoh, sebuah think tank pemungut pajak memiliki hubungan dengan Handgun Control, Inc. dan National Rifle Association, sehingga pengunjung dapat menemukan bahan penelitian yang relevan di kedua sisi masalah kontrol senjata. Internal Revenue Service (IRS) mengumumkan penyelidikan apakah tautan tersebut melanggar aturan untuk status bebas pajak. Menurut Anda, apa yang harus mereka simpulkan? Bagaimana berbagai kemungkinan keputusan oleh IRS mempengaruhi Web?
- 3.25 Perusahaan menjual spyware yang dapat mencegat dan merekam komunikasi telepon dan email pada berbagai layanan email. Perusahaan menjual perangkat lunak kepada lembaga pemerintah di Amerika Serikat (atau negara Anda, jika Anda berada di luar Amerika Serikat) yang menginginkannya untuk mengejar penjahat dan teroris. Menggunakan kriteria etika dari Bab 1 dan kriteria hukum atau konstitusional (dari Bab 2 maupun yang satu ini, atau berdasarkan konstitusi negara Anda jika Anda berada di luar Amerika Serikat), mengevaluasi keputusan untuk menjual perangkat lunak.
- 3.26 Dengan menggunakan kriteria etis dari Bab 1, evaluasi keputusan untuk menjual perangkat lunak yang dijelaskan dalam latihan sebelumnya kepada pemerintah yang represif.
- 3.27 Dalam Bagian 3.6, kami membahas argumen tentang proposal untuk biaya pengiriman konten lebih cepat melalui Internet. Menurut Anda, apa kemungkinan dampak dari tuduhan semacam itu? Alasan memberi. Gunakan analogi dari bidang lain.
- 3.28 Asumsikan Anda seorang profesional yang bekerja di bidang yang Anda pilih. Jelaskan hal-hal spesifik yang dapat Anda lakukan untuk mengurangi dampak dari dua masalah yang kita diskusikan dalam bab ini. (Jika Anda tidak dapat memikirkan apa pun yang terkait dengan bidang profesional Anda, pilih bidang lain yang mungkin menarik bagi Anda.)
- 3.29 Pikirkan ke depan untuk beberapa tahun ke depan dan jelaskan masalah baru, terkait dengan masalah dalam bab ini, kemungkinan berkembang dari teknologi digital atau perangkat.

Tugas-tugas

Latihan-latihan ini memerlukan beberapa penelitian atau kegiatan.

- 3.30 Cari tahu apakah perguruan tinggi Anda membatasi akses ke situs web apa pun dari sistem komputernya. Apa kebijakannya untuk menentukan situs mana yang dibatasi? Apa pendapat Anda tentang kebijakan itu?
- 3.31 Pada saat saya menulis ini, Facebook, dilarang di China sejak 2009, direncanakan untuk mendirikan kehadiran di sana. Itu harus mematuhi persyaratan dan persyaratan sensor China untuk memberikan informasi pengguna kepada pemerintah. Apakah Facebook sekarang ada di China? Jika demikian, bagaimana cara menanggapi persyaratan penyensoran dan pelaporan?

Latihan Diskusi Kelas

Latihan-latihan ini untuk diskusi kelas, mungkin dengan presentasi singkat yang dipersiapkan sebelumnya oleh kelompok-kelompok kecil siswa.

- 3.32 Berdasarkan undang-undang di Jerman yang melindungi privasi para penjahat yang telah menjalani hukuman mereka, seorang pembunuh mengambil tindakan hukum untuk memaksa Wikipedia menghapus artikelnya tentang kasusnya. Diskusikan konflik antara privasi dan kebebasan berbicara yang diangkat oleh kasus ini.
- 3.33 Sejauh mana materi kekerasan di Web dan di game komputer yang bertanggung jawab atas penembakan di sekolah? Apa yang harus dilakukan tentang hal itu, tanpa melanggar Amandemen Pertama?
- 3.34 Seorang manajer sistem komputer di sebuah universitas publik memperhatikan bahwa jumlah akses Web ke sistem melonjak secara dramatis. Sebagian besar akses yang ditingkatkan adalah ke halaman rumah satu siswa. Manajer sistem menemukan bahwa halaman rumahnya berisi beberapa gambar berorientasi seksual. Foto-foto itu mirip dengan yang diterbitkan di banyak majalah yang tersedia secara legal. Manajer sistem memberi tahu siswa untuk menghapus gambar. Seorang siswa perempuan yang mengakses gambar-gambar sebelum mereka dihapus mengajukan keluhan terhadap universitas karena pelecehan seksual. Siswa yang mengatur beranda mengajukan keluhan terhadap universitas karena melanggar hak Amandemen Pertama. Bagilah kelas menjadi empat kelompok: perwakilan untuk siswa perempuan, siswa laki-laki, dan universitas (satu kelompok untuk setiap keluhan). Seorang juru bicara untuk setiap kelompok menyajikan argumen. Setelah diskusi terbuka tentang argumen-argumen itu, ambillah suara kelas atas setiap keluhan.
- 3.35 Undang-undang CAN-SPAM berlaku untuk email komersial; pesan politik dikecualikan. Sekarang argumen bahwa undang-undang untuk membatasi atau mengatur spam harus memperlakukan kedua kategori email massal dengan cara yang sama. Presentasikan argumen untuk membenarkan perlakuan berbeda dari dua kategori ini.
- 3.36 Diskusikan pertanyaan di Bagian 3.3 tentang tanggung jawab etis untuk membuat situs web dengan informasi tentang bunuh diri untuk orang yang sakit parah yang kesakitan. Diskusikan pertanyaan analagis untuk membuat situs web dengan informasi tentang cara membuat bahan peledak untuk tujuan yang sah (mungkin pembongkaran atau pembersihan lahan pertanian). Jika jawaban berbeda untuk dua situasi, identifikasi atribut atau prinsip yang mengarah ke jawaban yang berbeda.
- 3.37 Setelah insiden serangan verbal jahat dan ancaman pembunuhan terhadap seorang blogger dari orang-orang yang tidak setuju dengan sesuatu yang ditulisnya, Tim O'Reilly dan Jimmy Wales mengajukan Kode Etik Blogger. Temukan salinan kode yang dikembangkan dari proposal ini (atau kode perilaku lain untuk blogger). Evaluasilah. Diskusikan kompatibilitasnya dengan kebebasan berbicara. Haruskah blogger mengikuti kode?
- 3.38 Apakah kontrol yang dimiliki perusahaan besar seperti Google atas hasil pencarian Internet merupakan ancaman terhadap kebebasan berbicara?
- 3.39 Haruskah Skype terus beroperasi di Cina di bawah joint venture dengan TOM, seperti yang dijelaskan dalam Bagian 3.5.2? Mengapa atau tidak?
- 3.40 (a) Dalam kerusuhan seperti yang terjadi di Inggris pada tahun 2011, di mana para perusuh merencanakan dan mengoordinasikan aktivitas mereka menggunakan (antara lain) BlackBerry Messenger, apakah Research In Motion (RIM) harus mematikan Messenger sementara? Asumsikan pemerintah tidak memiliki otoritas hukum untuk memerintahkan penutupan, tetapi lembaga penegak hukum dan pejabat pemerintah telah meminta RIM untuk menutup layanan untuk mencegah lebih banyak kekerasan.
(b) RUU cybersecurity di Senat AS (yang tidak lulus) memiliki ketentuan bahwa beberapa kritikus diyakini bisa memberikan otoritas pemerintah untuk mematikan Internet dalam keadaan darurat. Haruskah pemerintah memiliki otoritas seperti itu?
- 3.41 Aturan netralitas bersih yang dikeluarkan oleh FCC pada tahun 2011 memperlakukan jaringan komunikasi kabel dan nirkabel secara berbeda (memungkinkan lebih banyak fleksibilitas bagi operator jaringan nirkabel). Berikan beberapa alasan untuk memperlakukan mereka secara berbeda. Berikan beberapa alasan mengapa mereka harus diperlakukan sama. Menurut Anda apa yang paling masuk akal?

.

BUKU DAN ARTIKEL

Floyd Abrams, *Berbicara Secara Bebas: Percobaan Amandemen Pertama*, Viking Penguin, 2005

..

.

Lyrissa Barnett Lidsky, "Membungkam John Doe: Pencemaran Nama Baik dan Pengungkapan di Dunia Maya," Robert Corn-Revere, "Terperangkap di Web Seamless: Apakah Global Reach JurnalDuke Law, 49: 4, Februari 2000, hlm. 855– 946. (Tersedia di www.law.duke.edu.)

Membenarkan Kurang Kebebasan Berbicara? "Cato Institute, 24 Juli 2002

..

Rebecca MacKinnon, *Persetujuan dari Net-bekerja: Perjuangan di Seluruh Dunia untuk Internet Pusat Informasi Privasi Elektronik, Menyaring Kebebasan, Dasar*, 2012.

dan *Kebebasan 2.0: Perspektif Ucapan Bebas*

. pada Kontrol Konten Internet, www.epic.org, 2001

..

Evgeny Morozov, *The Delusion Net: Sisi Gelap Kebebasan Internet*, PublicAffairs, 2011

..

"Sains, Teknologi, dan Perubahan Pertama - Mike Godwin, *Hak Cyber: Membela Pidato Gratis di Era Digital*, Times Books, Random House, 1998

..

Marjorie Heins, *Tidak di Depan Anak-anak: "ketidaksenonohan," Sensor, dan Ketoleran*, Laporan Khusus, "Office of Technology Assessment, Departemen Perdagangan AS, Washington, DC, Januari 1988 (Laporan NO. OTA-CIT-369).

.

Pemuda, Hill & Wang, 2001

..

Scott Shane, *Pembongkaran Utopia: Bagaimana Informasi Berakhirnya Uni Soviet*, IR Dee, 1994. Nat Hentoff, *Pidato Gratis untuk Saya — Tapi Tidak Untuk*

. *Engkau: Bagaimana Orang Kiri dan Kanan Amerika dengan Tidak Memuji Bersama*, Harper Collins, 1992

..

Ithiel de Sola Pool, *Teknologi Kebebasan*, Harvard University Press, 1983. Buku ini menguraikan sejarah, hak, pembatasan, dan tanggung jawab berbagai komunika - Peter Huber, *Hukum dan Gangguan di Cyberspace*,

teknologi tions secara mendalam. Oxford Univ. Press, 1997. Mengkritik FCC

. pengaturan telekomunikasi, menunjukkan contoh-contoh di mana peraturan telah menunda pengenalan teknologi baru.

.

Eugene Volokh, "Kebebasan Berbicara di Dunia Maya dari Perspektif Pendengar: Pembatasan Pidato Pribadi, Libel, Tindakan Negara, Pelecehan, dan Seks," Univ. Anthony Lewis, *Kebebasan untuk Pemikiran Bahwa*

Chicago Legal Forum, 1996, hlm 377–436. Kami Benci: A Biografi Amandemen Pertama

., *Buku-buku Dasar*, 2008.

Tim Wu, *Saklar Utama: Kebangkitan dan Kejatuhan Kekaisaran Informasi*, Knopf, 2010.

1. Dari pidato oleh Mike Godwin di Carnegie Mellon

University, November 1994, dikutip dengan izin. (Pidato ini dikutip, termasuk bagian dari kutipan yang digunakan di sini, di Mike Godwin, "alt.sex.academic.freedom," *Wired*, Februari 1995, hlm. 72.) 2.

"Internet 2010 dalam Bilangan," Pingdom, [royal .pingdom .com](http://royal.pingdom.com) / 2011/01/12 / internet-2010-in-numbers, dilihat 22 November 2011.

3. Eric M. Freedman, "Pondering Pixelized Pixies,"

Komunikasi ACM, Agustus 2001, 44: 8 , hal. 27–29. 4. "Pengadilan Tinggi Aturan Hak Industri Kabel Lebih Besar Dari

Siaran," *Investor Bisnis Harian*, 28 Juni 1994. 5. Judul V, Bagian 230. 6. Iklan anggur di Internet dilindungi dalam kasus 2006 di Minnesota. Kasus-kasus sebelumnya menyangkut iklan tentang

tembakau, judi legal, suplemen vitamin, kandungan alkohol bir, harga obat resep, dan klaim Nike bahwa itu tidak menggunakan buruh sweatshop. Lee McGrath, "Sweet Nectar of Victory," *Liberty & Law*, Institute for Justice, Juni 2006, vol. 15, tidak. 3, hal. 1, 10. Robert S. Greenberger, "Lebih Banyak Pengadilan Mengeluarkan Iklan Perlindungan Amandemen Pertama," *Wall Street Journal*, 3 Juli 2001, hal. B1, B3. 7. Dalam *Kehidupan Voltaire*, Smith, Elder & Company, 1904. Lihat juga Fred S. Shapiro, ed., *The Yale Book of Quotations*, Yale University Press, 2007. Kutipan tersebut sering salah dikaitkan dengan Voltaire sendiri. 8. Gerard van der Leun, "Ini Adalah Wanita Telanjang," *Wired*, Premiere Issue, 1993, hlm. 74, 109. 9. Dick Thornburgh dan Herbert S. Lin, eds., *Pemuda, Pornografi dan Internet*, Akademi Nasional Tekan, 2002, books.nap.edu/catalog/10261.html. 10. Mike Godwin, "Sex, Cyberspace, dan Amandemen Pertama," *Laporan Kebijakan Cato*, Jan./Feb. 1995, 17 (1), hal. 10. 11. Robert Peck, dikutip dalam Daniel Pearl, "Pemerintah Mengatasi Lonjakan Smut di Internet," *Wall Street Journal*, 8 Februari 1995, hlm. B1. 12. Untuk komentar tentang banyak masalah dalam kasus ini, lihat Mike Godwin, "Virtual Community Standards," *Reason*, November 1994, hlm. 48–50. 13. Brian Roehrkasse, dikutip *Bloomberg News*, "AS Kebutuhanatas Data yang Dipertanyakan," *Los Angeles Times*, 26 Januari 2006, articles.latimes.com/2006/jan/26/business/fi-leahy26, dilihat 22 November, 2011. 14. Dalam *Brown v. Entertainment Merchants Association*, keputusan Mahkamah Agung membatalkan larangan California atas penjualan atau penyewaan video game kekerasan kepada anak di bawah umur, 2011. 15. Lolos sebagai Judul V dari Undang-Undang Telekomunikasi tahun 1996. 16. *Butler v Michigan*, 352 US 380 (1957). 17. Ajaran terhadap Mosi untuk Pidato Awal, *American Civil Liberties Union dkk. v. Janet Reno* (No. 96-963) dan *American Library Association et al. v. Departemen Kehakiman Amerika Serikat* (No. 96-1458). 18. *ALA v. Amerika Serikat*. 19. *Brown v. Entertainment Merchants Association*. 20. Brock Meeks, "Internet sebagai Teroris," *Pengiriman Cyberwire*, 11 Mei 1995, cyberwerks.com/cyberwire/cwd/cwd.95.05.11.htm. Brock Meeks, "Target: Internet," *Komunikasi ACM*, Agustus 1995, 38 (8), pp. 23–25. 21. Kutipan dalam paragraf ini berasal dari Meeks, "Internet sebagai Teroris." 22. David Armstrong, "Resep Bom Berkembang Online Meskipun Hukum Baru," *Wall Street Journal*, 18 Januari 2001, hal. B1, B8. Seorang pria menerima tawar-menawar pembelaan selama satu tahun di penjara. 23. Amol Sharma, "Operator Nirkabel Mengatur Standar Ketat Ketat untuk Konten," *Wall Street Journal*, 27 April 2006, hlm. B1, B4. 24. Dewan Rating Perangkat Lunak Hiburan, www.esrb.org. 25. www.missingkids.com. 26. Dalam putusan yang menjatuhkan Pornografi Anak UU Pencegahan (Ashcroft v. Speech Speech Gratis). Lebih banyak argumen menentang hukum ada dalam Friedman, "Merenungkan Pixelized Pixies." Argumen di sisi lain muncul di Foster Robberson, "Pornografi Anak Virtual di Net Tidak Lebih Sedikit Dari Hal Nyata," *Arizona Republic*, 28 April 2000, p. B11. 27. John Letzing, "'Spam King' Surrenders," *Wall Street Journal*, 4 Agustus 2011, online.wsj.com/article/BT-CO-20110804-726251.html, dilihat 23 November 2011. 28. *Intel Corporation v. Hamidi*, news.findlaw.com/wp/docs/intel/intelhamidi63003opn.pdf, dilihat 22 Oktober 2011. 29. Jayson Matthews, "Harris Interactive Continues Spam Battle with MAPS," siliconvalley.internet.com/news/article/0,2198,3531_434061,00.html, 9 Agustus 2000, dilihat 9 April 2001. 30. Dikutip dalam Tom Espiner, "Antispam Group Menolak Rencana Pembayaran E-Mail," *CNET News*, news.com 7 Februari 2006, dilihat 27 November 2011. 31. Nama lengkapnya adalah Mengendalikan Penyerangan Undang-undang Pornografi dan Pemasaran Tidak Dipertahankan. 32. Federal Trade Commission, "CAN-SPAM Act: Panduan Kepatuhan untuk Bisnis," September 2009, business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business, dilihat 22 Oktober 2011. 33. John Simons, "Peraturan CFTC tentang Penerbitan Hancur," *Wall Street Journal*, 22 Juni 1999, hlm. A8. Scott Bullock, "Penyerahan CFTC tentang Perizinan Lisensi," *Liberty & Law*, Institute for Justice, April 2000, 9: 2, hlm. 2. 34. Swedenburg v. Kelly. 35. Dikutip dalam Brad Stone, "Web Gurus Bertujuan untuk Membawa Sipil ke Blogosfer Buruk-Tempered," *New York Times*, 9 April 2007, www.technewsworld.com/story/56774.html, dilihat 21 Juni, 2007. 36. Seseorang atau organisasi yang menggunakan nama foia.org membocorkan email penelitian iklim. (FOIA adalah

akronim untuk "Freedom of Information Act.") Saya membaca beberapa (tidak semua) dokumen di foia2011.org/index.php?id=402. Saya membaca banyak artikel dengan kutipan dari email dan tanggapan dari para peneliti CRU. "University of East Anglia Emails: Kutipan Paling Bersaing," The Telegraph, 23 November 2009, www.telegraph.co.uk/earth/environment/Exercises 178

globalwarming / 6636563 / University-of-East-Anglia- email-the-most-contentious-quotes.html, dilihat 27 November 2011. Antonio Regalado, "Unit Penelitian Iklim Mematahkan Hukum Informasi Inggris," Science, 28 Januari 2010, news.sciencemag.org/scienceinsider/2010/01/climate-research.html, dilihat 23 Desember 2011. Larry Bell, "Climategate II: Senjata Merokok Lebih dari Pembentukan Pemanasan Global," Forbes, 29 November 2011, www.forbes.com/sites/larrybell/2011/11/29/climategate-ii-lebih-merokok-senjata-dari-global-pemanasan-pendirian, dilihat 23 Desember 2011. "Cherry-Picked Phrases Dijelaskan," University of East Anglia, 23 November, 2011, www.uea.ac.uk/mac/comm/media/press/CRUstatements/rebuttalsandcorrections/phrasesmenjelaskan, dilihat 23 Desember 2011. 37. Tim Lister, "WikiLeaks Daftar Situs Kunci Keamanan AS," CNN AS, 6 Desember 2010, artikel.cnn.com/2010-12-06/us/wikileaks_1_wikileaks-founder-julian-assange-diplomat-tanah-air-keamanan?_s=PM:AS, dilihat 20 Agustus 2011. Tim Lister dan Emily Smith, "Banjir WikiLeaks Kabel Mencakup Identitas Puluhan Insan," CNN US, 31 Agustus 2011, artikel.cnn.com/2011-08-31/us/wikileaks.sources_1_diplomatic-cables-wikileaks-websites?_S=PM:AS, dilihat 22 Oktober 2011. 38. Die Welt, dikutip dalam Floyd Abrams, "Don't Cry for Julian Assange," Wall Street Journal, 8 Desember 2011, online.wsj.com/article/SB10001424052970204323904577038293325281030.html, dilihat 26 Desember 2011. 39. McIntyre v. Komisi Pemilu Ohio, 514 US 334, 115 S.Ct. 1511 (1995). 40. Jeffrey M. O'Brien, "Agen Bebas," Wired, Mei 2001, hal. 74. 41. Neil King, "Start-Up Kecil Membantu CIA Mask Its Bergerak di Web," Wall Street Journal, 12 Februari 2001, pp. B1, B6. 42. Declan McCullagh, "Klaim Bertolak Holes SafeWeb," Wired News, 12 Februari 2002, www.wired.com/news/politics/0,1283,50371,00.html. 43. Dikutip dalam Robert Corn-Revere, "Terperangkap dalam Web Seamless: Apakah Internet Global Reve Justify Less Freedom of Speech?" Bab dalam Adam Thierer dan Clyde Wayne Crews Jr., eds. Siapa yang Mengatur Net? Tata Kelola Internet dan Yurisdiksi, Cato Institute, 2003. 44. Peter L. Bernstein, Melawan Dewa: Kisah Resiko yang Luar Biasa, John Wiley & Sons, 1996, hlm. 89. 45. Louisa Lim, "China untuk Menyensor Pesan Teks," BBC News, 2 Juli 2004, news.bbc.co.uk/2/hi/asia-pacific/3859403.stm. 46. Untuk informasi lebih lanjut tentang bagaimana pemerintah menggunakan Internet untuk menggagalkan gerakan kebebasan, lihat Evgeny Morozov, The Net Delusion: Sisi Gelap Kebebasan Internet, PublicAffairs, 2011. 47. Barry Bearak, "Taliban Akan Mengizinkan Akses ke Penjara Pekerja Bantuan Kristen," New York Times, 26 Agustus 2001, www.nytimes.com/2001/08/26/world/taliban-akan-mengizinkan-akses-ke-penjara-christian-aid-workers.html?pagewanted=all&src=pm, dilihat 26 Nov. 2011. 48. Dalam "Google Meluncurkan Versi Disensor Search Engine-nya," 25 Januari 2006, www.rsf.org. 49. Elinor Mills, "Google ke Censor China Web Searches," CNET News.com, 24 Januari 2006, news.com.com/Google+ke+censor+China+Web+search/2100-1028_3-6030784.htm. 50. Dikutip dalam L. Gordon Crovitz, "Teman Baru Baru dari Facebook," Wall Street Journal, 2 Mei 2011, online.wsj.com/article/SB10001424052748703567404576293233665299792.html, dilihat 27 November 2011. 51. Dikutip dalam Jennifer Valentino-DeVries, Julia Angwin, dan Steve Stecklow, "Dokumen Mengungkap Metode Surveilans," Wall Street Journal, 19 November 2011, online.wsj.com/article/SB10001424052970203611404577044192607407780.html, dilihat 26 November 2011. 52. "Pernyataan tentang Interupsi Layanan Nirkabel Sementara di Stasiun-stasiun Pilih BART pada 11 Agustus," BART, 12 Agustus 2011, www.bart.gov/news/articles/2011/news20110812.aspx, dilihat 22 Oktober 2011. Lihat juga Geoffrey A. Fowler, "Telepon Cutoff Mengusir Kekhawatiran Tentang Batas Berbicara," Wall Street Journal, 16 Agustus 2011, online.wsj.com/article/SB10001424053111904253204576510762318054834.html, dilihat 18 Oktober 2011. 53. Dikutip dalam Fowler, "Phone Cutoff Stirs Worry." 54. Alan Davidson, "Vint Cerf Berbicara tentang Netral Netity," Google Blog, googleblog.blogspot.com/2005/11/vint-cerf-speak-out-on-net-neutrality.htm, 8 November 2005. 55. Maret 2006, dikutip di situs web Hands Off the Internet, handsoff.org, dilihat 31 Juli 2006. 56. Armstrong, "Resep Bom Yang Berkembang Online Meskipun Ada Hukum Baru." 57. Robert D. Atkinson, "Meratakan Bidang Bermain E-Commerce: Memastikan Pajak dan Kewajiban Pengaturan untuk Bisnis Online dan Offline," Progressive Policy Institute, www.ppionline.org, 30 Juni 2003. 58. Massimo Calabresi, "Cepat, Sembunyikan Tank!" Waktu, 15 Mei 2000, hal. 60.

Soal dan Penyelesaian berdasarkan Materi Bab 3 “Kebebasan Berbicara”

1. Sebutkan tiga kategori untuk perlindungan Amandemen Pertama dan peraturan pemerintah dari media komunikasi yang dikembangkan di Amerika Serikat pada abad ke-20.

Ketiga kategori tersebut adalah:

- ✓ Media cetak (surat kabar, buku, majalah, pamflet)
- ✓ Siaran (televisi, radio)
- ✓ Operator umum (telepon, telegraf, dan sistem pos)

2. Video game semakin banyak jenisnya tersebar di lingkungan masyarakat khususnya anak-anak sebagai peminat tertinggi. Bagaimana video game dapat menjadi ancaman bagi kepribadian seorang anak?

- ✓ Video game dapat menjadi ancaman bagi kepribadian seorang anak apabila mengandung konten kasar yang “berdarah” dalam artian beberapa video game menggambarkan pembunuhan dan penyiksaan; beberapa fokus pada kekerasan terhadap perempuan dan anggota kelompok etnis dan agama tertentu. Hal tersebut tentunya akan membuat seorang anak penasaran melakukan tindakan seperti yang ada pada video game karena seorang anak masih belum mampu untuk memilah ataupun memutuskan suatu tindakan yang benar untuk dilakukan sehingga dalam hal ini diperlukan peranan orangtua dan juga pemerintah dalam memfilter konten yang layak untuk dipublikasikan bagi seorang anak.

3. Pada tahun 1973, Mahkamah Agung, di *Miller v. California*, menetapkan tiga kriteria untuk menentukan apakah suatu materi tidak senonoh menurut hukum. Coba jelaskan kriteria tersebut.

Kriteria tersebut adalah

- ✓ menggambarkan tindakan seksual (atau ekskretori) yang penggambarannya secara khusus dilarang oleh hukum negara bagian.
- ✓ Penerapan standar komunitas, maksudnya adalah untuk menghindari masalah menetapkan standar nasional kecabulan di negara yang begitu besar dan beragam.
- ✓ Tidak memiliki nilai sastra, seni, sosial, politik, atau ilmiah yang serius.

4. Coba jelaskan menurut pemahaman Anda mengapa memposting, menjual, dan membocorkan materi sensitif di suatu media dapat menimbulkan masalah yang besar?

- ✓ membocorkan materi sensitif di suatu media dapat menimbulkan masalah yang besar dikarenakan hal tersebut dapat menjadi penyebab awal terjadinya masalah sosial dan etika termasuk masalah hukum yang dapat merugikan pihak-pihak tertentu karena adanya kebocoran informasi yang jika dibiarkan dapat jatuh ke tangan yang salah dan akan digunakan sebagai alat dalam memulai tindak kejahatan bisa saja berupa perang politik atau terorisme.

5. Coba jelaskan perbedaan penggunaan anonimitas yang positif dan negatif.

- ✓ Penggunaan anonimitas secara positif dapat digambarkan dengan banyak orang yang menggunakan browser Web anonim adalah untuk perlindungan bagi individu. Melindungi privasi, melindungi terhadap pencurian identitas dan profil konsumen, dan melindungi terhadap pemerintah yang menindas. Namun, bisnis, lembaga penegak hukum, dan dinas intelijen pemerintah jugadapat menggunakan browser web anonim untuk menyimpan penelitian dan perencanaannya tentang rahasia produk baru dari pesaing. Penggunaan Web Anonim juga membantu penyelidikan penegakan hukum. Misalkan agen penegak hukum mencurigai sebuah situs berisi pornografi anak, informasi teroris, materi yang melanggar hak cipta, atau hal lain yang relevan dengan investigasi. Jika mereka mengunjungi situs tersebut dari komputer departemen mereka, mereka mungkin diblokir atau melihat halaman hambar dengan tidak ada yang ilegal.
- ✓ Penggunaan anonimitas secara negatif dapat digambarkan dengan banyaknya orang yang juga menggunakannya untuk penipuan, pelecehan, dan pemerasan, untuk mendistribusikan pornografi anak, untuk mencemarkan nama baik atau mengancam orang lain dengan bebas hukuman, mencuri dokumen bisnis rahasia atau informasi kepemilikan lainnya, dan melanggar hak cipta. Postingan anonim dapat menyebarkan desas-desus palsu yang secara serius merusak bisnis, memanipulasi saham, atau menghasut kekerasan. Anonimitas membuat sulit untuk melacak pelaku kesalahan. Seperti enkripsi, teknologi anonimitas menimbulkan tantangan bagi penegak hukum. Anonimitas dapat menyamarkan pengawasan ilegal oleh lembaga pemerintah atau pengawasan legal namun reaktif di negara-negara yang tidak bebas.