PRIVACY ENGINEERING DALAM TEKNOLOGI DIGITAL RIGHT MANAGEMENT

Yosef Sukianto – NIM : 13506035

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
Email : if16035@students.if.itb.ac.id

Abstrak

Perkembangan teknologi Internet yang pesat sekarang ini khususnya dalam distribusi konten (produk dan jasa) berbasis Internet merupakan peluang yang besar bagi kalangan produsen, distributor dan konsumen untuk mendapatkan manfaatnya masing - masing. Namun di sisi lain dapat mengancam privacy bagi para penggunanya. Masalah privacy yang sering timbul biasanya gangguan pada tahapan transaksi bisnis (misal kasus pada industri credit card), namun masalah baru dan lebih serius akan dijumpai pada perkembangan selanjutnya. Teknologi atau sistem yang selama ini digunakan untuk mengatasi masalah keamanan & privacy (misal, enkripsi, anonimitas, pseudonimitas, dll) sepertinya kurang efektif dan perlu pengembangan lebih lanjut dalam melindungi hak-hak stakeholder.

Dalam tulisan ini kami memaparkan kontribusi teknologi DRM dalam mengkompromikan dan melindungi privacy penggunanya. DRM adalah suatu terminologi yang melingkupi beberapa teknologi yang digunakan untuk menetapkan penjelasan pendahuluan akses kendali terhadap software, musik, film dan data digital lainnya. DRM menangani pendeskripsian, layering, analisis, valuasi, perdagangan dan pengawasan hak dalam segala macam aktivitas digital.

Akan dijelaskan pula salah satu prinsip DRM yang mudah untuk diimplementasikan dan secara potensial cukup efektif yakni privacy engineering untuk mengatasi masalah keamanan dan privacy bagi produsen, distributor dan konsumen sebagai para penggunanya. Kesemua keuntungan pihak yang terlibat diharapkan dapat memberikan dampak positif secara makro maupun mikro dunia industri.

Kata kunci: *Digital Right Management, Privacy Enginering, Costumizable Privacy..*

PENDAHULUAN

Perkembangan teknologi digital, khususnya Internet yang pesat sekarang menimbulkan apa yang disebut sebagai “masalah dua mata pedang”, di satu sisi menjadi peluang positif bagi kalangan produsen, distributor dan konsumen untuk mendapatkan manfaat dan keuntungannya, di sisi lain menjadi ancaman baru dalam hal distribusi konten (produk dan jasa) berbasis Internet bagi stake holder-nya. Ancaman tersebut yang paling umum dan signifikan yakni masalah privacy (hak cipta, kepemilikan, kekayaan intelektual, dan hak lisensi). Masalah privacy timbul dikarenakan mudahnya pencopy-an/ penggandaan atau pencetakan material /kontent suatu produk. Pada Digital Right Managemen (disingkat DRM) generasi sebelumnya, materi produk hanya bias diakses atau dimiliki oleh pihak yang membayarnya, dengan pesatnya teknologi Internet pihak-pihak yang tidak berwenang tau tidak memiliki hak pun bisa mendapatkannya dengan mudah. Masalah/ancaman yang tipikal yakni kasus pada saat berlangsungnya transaksi bisnis sebagai contoh pada kasus transaksi dengan kartu kredit.Namun, sejalan dengan kepesatan teknologi, masalah yang lebih rumit dan butuh kerja yang luar biasa, tak lama akan kita jumpai. Ancaman terhadap distribusi konten (suatu produk atau jasa) dapat ditanggulangi oleh suatu manajemen khusus, yang disebut Digital Right Manajamen. Teknologi atau sistem yang selama ini digunakan untuk mengatasi masalah keamanan & privacy (misal, enkripsi, anonimitas, pseudonimitas, dll) sepertinya kurang efektif dan perlu pengembangan lebih lanjut dalam melindungi hak-hak stakeholder. Dalam tulisan ini akan dipaparkan salah satu prinsip DRM yang mudah untuk diimplementasikan dan secara potensial cukup efektif

yakni privacy engineering untuk menangani masalah tersebut.

DRM

1. Definisi DRM

DRM adalah suatu terminologi yang melingkupi beberapa teknologi yang digunakan untuk menetapkan penjelasan pendahuluan akses kendali terhadap software, musik, film dan data digital lainnya. DRM menangani pendeskripsian, layering, analisis, valuasi, perdagangan dan pengawasan hak dalam segala macam aktivitas digital.

2. Teknologi Keamanan dalam DRM

Sebagai pengetahuan, berikut ini adalah beberapa teknologi keamanan yang berkaitan dengan DRM, diantaranya:

- Keamanan dan Integritas Fitur suatu Sistem Operasi Komputer
- Right- Management Language
- Enkripsi
- Tandatangan Digital
- Fingerprinting, dan teknologi "marking" lainnya.

3. Membangun DRM

Sistem DRM dibangun dengan menyatukan teknologi keamanan dalam satu bundel system end-to-end yang melayani kepentingan dan kebutuhan pemilik, distributor, pengguna dan pihak terkait lainnya.

Dalam membangun RMdiperlukan dua arsitektur kritis yang perlu dipertimbangkan. Pertama adalah arsitektur fungsional yang melingkupi modul atau komponen tingkat tinggi yang secara bersama-sama akan membentuk system end-to-end. Kedua adalah aristektur informasi yang melingkupi pemodelan entitas-entitas dalam DRM dan hubungan antara entitas-entitas tersebut.

a. Arsitektur Fungsional

Kerangka kerja keseluruhan DRM dapat dimodelkan dalam tiga area bahasan:

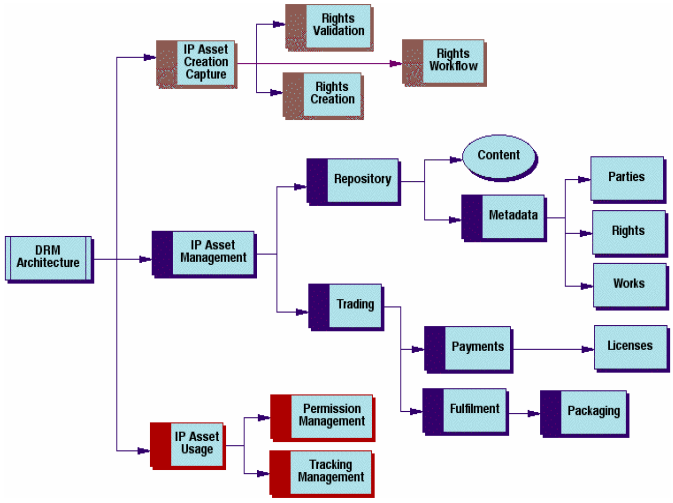
- Intellectual Propierty (IP) Asset Creation and Capture: yakni suatu cara untuk mengelola pembuatan/kreasi suatu konten sedemikian hingga mudah untuk diperjual-belikan.
- IP Asset Management: yakni suatu cara untuk mengelola dan memperjual-belikan konten. Termasuk di dalamnya menerima suatu konten dari creator/pembuat kedalam suatu sistem manajemen asset.
- IP Asset Usage: yakni bsuatu cara untuk mengelola penggunaan konten pada saat pertama kali diperjual-belikan. Termasuk di dalamnya mendukung kendala-kendala yang terjadi pada perdagangan konten dalam suatu system desktop /software tertentu.

b. Arsitektur Informasi

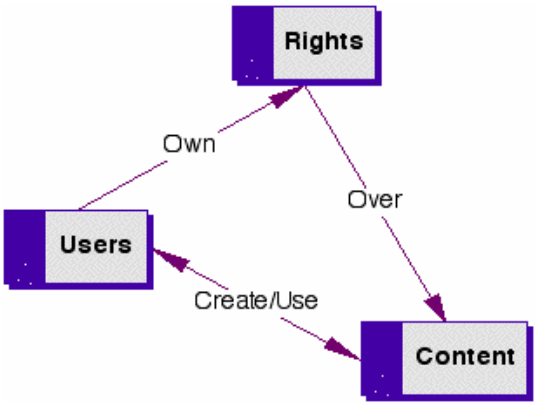
Arsitektur ini berhubungan dengan bagaimana cara agar entitas-entitas yang ada dibuat modelnya dalam kerangka kerja keseluruhan DRM berikut hubungan/relasi di antaranya. Bahasan yang penting mengenai kebutuhan yang diperlukan untuk membangun model Informasi DRM yakni:

- Pemodelan entitas- entitas
- Pengidentifikasi dan Pemaparan entitas- entitas
- Pengekspresian pernyataan hak hak.

Berikut adalah skema dua arsitektur kritis DRM



Gambar 1: Arsitektur Fungsional DRM



Gambar 2: Arsitektur Informasi DRM
Model Entitas Inti

diambil dalam mengelola suatu konten, seperti disebutkan pada bagian pendahuluan, tugas kita yakni memikirkan/memberi solusi untuk meminimalisasi dari penyalah gunaan hak pihak yang terlibat. DRM bukanlah suatu system yang sempurna, dalam arti dapat mengatasi segala macam persoalan mengenai hak-hak digital pemilik, distributor dan pengguna. Yang hendak ditawarkan di sini adalah bahwa teknik DRM yakni privacy engineering dapat memberikan pengaruh/dampak pada privacy penggunanya dan agar supaya teknik ini dapat diterapkan dalam setiap tahapan system DRM, baik perancangan, pembangunan dan pendayagunaan. Dari arsitektur informasi DRM dapat dijelaskan adanya hubungan yang saling melekat antara penegakkan copyright sang pemilik dan distributor yang membangun system DRM dan privacy penggunanya. Penegakkan hak (Rights Enforcment) dapat difasilitasi dengan menselusur jejak penggunanya (user tracking) atau kontrok jaringan komputer penggunanya, namun kedua hal tersebut secara potensial merusak privacy pengguna. Salah satu cara yang sering digunakan tanpa merusak privacy yakni dengan mengumpulkan data pada level distributor atau operator jaringan. Namun kita butuh fitur dan teknik baru untuk mengatasai ancaman yang terus berkemabng dan meningkat dalam perlindungan konten.

4. Strategi DRM

Ada beberapa strategi DRM yang berbeda-beda, baik model atau efek bagi privacy penggunanya. Salah satu strategi yang biasa disebut persistent distribution, yakni melengkapi meta data DRM dengan konten digital dimana dalam transaksi dasar disebutkan di atas, bahwa setiap produk digital yang ada dalam situs distributor diformat hanya untuk penggunaan saja (bukan copy atau distribusi ulang) dan dapat digunakan dengan suatu program aplikasi persetujuan tertentu. Dan setiap aplikasi tersebut dapat menginterpretasikan metadata DRM distributor berikut kontennya. Setiap file yang didownload, termasuk di dalamnya konten berikut metadata yang menjelaskan mengenai hak-hak yang diterima oleh pengguna. Suatu konten dan hak-hak tidak harus didownload dari situs yang sama; maksdunya adalah, dalam strategi umum DRM, kedua hal tersebut (konten dan hak-hak) masing-masing ditransfer hanya satu kali ke pengguna yang kemudian keluar dari pengawasan distributor. Dengan menggunakan program aplikasi persetujuan, pengguna hanya dapat mengakses konten sesuai dengan yang dijelaskan dalam metadata hak-hak.

Contoh persetujuan untuk file teks, yaitu, bahwa teks tersebut hanya dapat dibaca atau dicetak, namun tidak bisa untuk disunting atau distribusi ulang. Musik promosi ataupun video hanya dapat diputar untuk sebanyak jumlah terbatas. Dalam strategi ini, metadat hak hak ditambahkan pada informasi engenai pengguna yang dapat dikumpulkan atau ditambang. Sedemikian hingga, strategi ini tidak berdampak pada privacy pengguna.

Industri yang menggunakan strategi di atas yakni, Apple dengan iTunes Music Store, , yang menjual online lagu seharga $0.99, dana dapat mengcopy lagu tersebut ke dalam CD tanpa pembatasan dan mentransfernya ke dalam iPods juga tanpa pembatasan. Lagu/musik yang dibeli dalam bentuk / format file AAC yang didukung oleh alat/devais iPods, dan DRM diaplikasikan dengan apa yang disebut FairPlay. Banyak devais musik yang tidak cocok/kompatibel dengan format AAC dan hanya iPod sendiri yang dapat memutar file format tersebut. Apple juga mencadangkan hak untuk mengubah pemabatasan DRM pada musik yang telah didownload. Sebagai contoh, barubaru ini Apple memutuskan untuk membatasi jumlah pengcopyan playlist dari sepuluh kali ke tujuh kali. Lagu lagu yang didownload hanya dapat diputar pada lima komputer pada suatu waktu, dan pengguna tidak dapat menyunting lagu yang telah dibeli.

Staregi lainnya, yaitu dengan pengguna hanya dapat mengakses file dengan nomor serial atau menggunakan alat khusus untuk menjalankan file yang didownload. Distributor akan

memberikan update untuk penggunaan konten yang lebih lama (tentu setalah melakukan pembayaran).

Industri yang memanfaatkan strategi ini, selain Apple yang disebutkan sebelumnya, yaitu Norman Anti Virus, dimana pengguna dapat mendownload versi trial/coba Anti Virusnya, dengan mengisi informasi pengguna (misal, alamat email pengguna), kemudian akan memberikan kode aktivasi (nomor serial) ke alamat email pengguna dan hanya bisa digunakan selama 30 hari. Namun untuk update anti virus terbaru, pengguna harus membeli kode aktivasi update tersebut.

Strategi yang ketiga, yakni, apabila pengguna setelah mendownload file/konten dari suatu distributor (yang legal), maka ia dapat menggunakan konten tersebut disetiap saat dan pada segala macam devais yang berfungsi (setelah melakukan pembayaran). Strategi ini memerlukan proses penjejakan yang lebih komplek disbanding strategi lainnya, dimana informasi dan data pengguna akan dipantau, termasuk catatan kapan pengguna selesai mendengarkan, membaca atau menampilkan history-nya. Hal ini secara kualitatif merupakan ancaman yang lebih serius dibandingkan dengan apa yang telah disebutkan sebelumnya.Dimana akan diketahui file apa yang telah didownload, apakah video pornografi, dan berapa kali video tersebut ditonton/diputar.

Ada yang mengatakan bahwa menjual barang digital/secara digital lebih banyak kerugian dibandingkan keuntungannya, namun dengan era Internet dan digital sekarang ini, akan mundur ke belakang apabila kita tidak memanfaatkannya, dan kerugian yang ditimbulkannya dapt direduksi dengan menggunakan teknik, atau metodelogi yang lebih canggih dan menyeluruh. Misalkan adalah DRM. Seperti dijelaskan sebelumnya, beberapa ancaman potensial terhadap privacy disebabkan oleh distribusi berbasis Web bukan semata oleh DRM. Namun juga perlu dicatat, bahwa distribusi berbasis Web lebih kondusif terhadap privacy penggunanya dibandingkan dengan jalur distribusi lama.

DRM diperlukan untuk mengatasi ataupun melengkapi dan menambal celah yang terbuka dari penggunakan kryptograpi. Seperti kita ketahu dengan semakin berkembangnya industri dan teknologi perangkat keras dan perangkat lunak, secanggih apapun program kryptograpi/persandian masih dapat ditembus dan diketahui cara penggunaan konten digital secara illegal.

PRIVACY ENGINERING (PE)

Dalam bagian ini akan dibahas mengenai beberapa aspek yang berkaitan dengan bagaimana privacy engineering diperlukan untuk memberikan solusi atas masalah yang biasa dihadapi oleh DRM konvensional, namun terbih dahulu akan dijelaskan aspek dasar/latarbelakang dari penggunaan PE.

1. **Aspek dasar/latar belakang PE**
   Latar belakang digunakannya PE sebagai suatu jawaban atas apa yang muncul dalam transaksi bisnis yang berbasis Internet atau distribusi kontent dengan pasar yang massal yang secara spesifik dibentuk oleh DRM. Sebagai contoh, suatu model distribusi yang tidak menggunakan DRM, misalkan pada transaksi dasar, dimana pengguna mendownload suatu produk digital dari situs web (disebut situs) distributor; transaksi tersebut bisa atau tidak melibatkan pembayaran, dan apabila melibatkan , maka pengguna akan menggunakan kartu kredit atau informasi pribadi lainnya yang memungkinkan proses pembayaran terlaksana yang pada akhirnya pengguna mendapatkan produk digital tersebut dan menggunakan sesuai yang dia inginkan. Ada dua hal utama dari transaksi tersebut yang dapat menjadi ancaman dari sisi privacy pengguna. Pertama (yang merupakan tipikal dari kebanyakan perdagangan berbasis Web), aktifitas Web-nya terawasi (misal, cookies client, log server, dll). Kedua, yakni, data kartu kredit atau pembayaran lainnya dapat diketahui pihak lain. Namun kedua ancaman tersebut tidak ada kaitannya dengan konten itu sendiri. Mengacu pada contoh kasus di atas, DRM diperlukan pada saat pasca download terjadi, yakni pada setelah konten tersebut sudah berpindah tangan, dari pemilik ke distributor ke pembeli/pengguna akhir. Dalam tulisan ini, DRM yang dimaksud yakni produksi atau reproduksi dalam jumlah besar (mass production).

2. **Aspek ekonomi dari PE**
   Salah satu alasan ekonomi para pebisnis menggunakan infrastruktur Internet yakni untuk mendapatkan keuntungan biaya dibanding pesaingnya. Sebagaimana disebutkan dalam hukum Metcalfe, PE diperlukan untuk mengatasi permasalahan yang ada dalam infrastruktur

Internet yakni jaringan. Pebisnis menggunakan Internet untuk mendapatkan keuntungan besar dengan mereduksi biaya. Namun di sisi lain, privacy penggunanya belum dapat diatasi dengan sempurna.

3. Insentif bisnis

Dua isu utama pebisnis berkaitan dengan praktek dalam hal privacy: mengapa informasi pengguna harus dikumpulkan, dan mengapa privacy tidak perlu ditawarkan. Ada alasan yang resmi bagi pebisnis untuk mengumpulkan data dan informasi, seperti retensi pelanggan, statistic, manajemen resiko, kostumisasi, dan pembayaran (billing). Sebagai contoh, operasi pada jaringan (network) dapat (dan mungkin juga harus) mengumpulkan data penggunaan untuk pemodelan traffic. Pemodelan traffic Internet adalah masalah yang besar dan serius, tanpa pemodeln yang baik, lalu lintas Internet akan berdampak pada penurunan kinerja, kualitas pelayanan, dlsb. Oleh karena itu pengumpulan datapenggunaans sangat diperlukan untuk pemodelan traffic Internet. Dalam distribusi konten dan kaitannya dengan DRM, operator jaringan ingin mengetahui darimana suatu konten tertentu diakses, terutama pada konten kualitas tinggi (misal multimedia, video dan suara) dalam rangka untuk mendistribusikan replica cache sehingga dapat menghemat penggunaan bandwidth, latency-reducing, penyesuaian beban (load-balancing). Sebagai contoh, penyedia konten memerlukan data bahwa berapa banyak suatu lagu diakses untuk menghitung kompensasi bagi pemilik (artis atau pemegang hak cipta).

Pebisnis juga memiliki hak untuk tidak membuka/menawarkan privacy. Karena nilai dari informasi itu sendiri yang sulit dan tentunya mahal.

Pendekatan untuk penerapan praktis PE Dalam penerapan praktis PE di dunia nyata, dapat menggunakan pendekatan yang ditawarkan oleh [1] yaitu : (a) Fair Information Principle dan cara implementasinya, dan (b) yakni kebutuhan aka audit privacy dan penegakkan kebijakan mengenai privacy.

a. Fair Information Principle (FIP) atau Prinsip Informasi yang Jelas, adalah suatu kerangka kerja untuk memeriksa koleksi dari informasi yang termasuk dalam area sensitif akan privacy, sepert pada area perawatan kesehatan. FIP telah banyak digunakan dalam rangka mencapai tujuan privacy yang diinginkan. Varian dari prinsip tersebut berpijak pada hukum perlindungan privacy . FIP melingkupi petunjuk-petunjuk, diantaranya:

- Batasan pengumpulan data
- Keakurasian data
- Pembatasan penggunaan
- Keamanan
- Keterbukaan
- Partisipasi
- Akuntabilitas Organisasi.

Yang membedakan antara FIP dengan kryptograpi adalah, dalam petunjuknya, FIP tidak menggunakan pendekatan teknologi dan lebih pada penggunaan tujuan yang umum. Sedangkan kryptograpi menggunakan pendekatan teknologi informasi privacy atau perhitungan komputasi. FIP cukup penting, dikarenakan tidak semua bisnis dapat mengadopsi pendekatan teknologi, sehingga perlu pendekatan non teknologi.

yang tidak membutuhkan perangkat lunak tertentu untuk menjaga privacynya, seperti penggunaan cookies blocker, yang berarti penggunaan perangkat lunak privacy (privacy – respectingsoftware) kebanyakan gagal diterapkan. Rata-rata pengguna tidak mau membayar atas suatu produk digital, sehingga killer application seperti Napster diterima oleh jumlah besar pengguna (walaupun akhirnya dituntut oleh produesn dan distributor). Oleh karena itu seperti disarankan pada [1], perlu adanya pendekatan alternatif dari PE untuk menghindari kegagalan penggunaan perangkat lunak privacy, yaitu:

1. Perlu diterapkan prinsip-prinsip FIP
2. Privacy dibundel dalam satu teknologi DRM. Konsumen tidak diberi tugas tambahan untuk melindungi privacy-nya.
3. Biaya yang rendah untuk membundel privacy dalam DRM
4. Biaya yang rendah bagi konsumen untuk menggunakan bundel privacy dalam suatu DRM. Biaya itu termasuk biaya moneter pelayanan dan kemudahan penggunaan, latency, dan hal-hal mengenai “pengalaman penggunaan” lainnya.

FIP dapat diterapkan dalam DRM, dikarenakan, sesuai dengan hukum yang berlaku di banyak Negara, Asia, Eropa dan banhkan Amerika, dan selain itu FIP juga merupakan standar penggunaan yang praktis.

b. Prinsip sederhana untuk PE Setelah mengetahui secara konseptual apa dan bagaimana FIP diterapkan dalam DRM , selanjutnya yakni ,bagaimana mengkonversi FIP ke dalam bentuk prinsip engineering. Dalam bagian ini akan dijelaskan singkat mengenai system arsitektur, system engineering, penggunaan prinsip teknologi skala rendah, dan penggunaan prinsip non teknologi sedemikian hingga tercapai tujuan disribusi dan DRM Adapun penjelasannya adalah sebagai berikut:

Costumizable Privacy, dengan maksud bahwa suatu system DRM harus dapat dikonfigurasi untuk mengakomodasi kebutuhan, proses pengumpulan informasi dan prosedur penanganannya.

Collection Limitation, dengan maksud bahwa suatu bisnis perlu menentukan informasi apa saja yang dibutuhkan untuk diambil untuk keeperluan bisnis, dan integrasi system kelegalan. Sebagai contoh, system keamanan kartu kredit memeerlukan transfer suatu informasi alamat pembayaran (billing). Tidak semua aplikasi memerlukan Informasi Pengidentifikasian Pribadi (PII: Personal Identifying Personal). Dalam system DRM, perlu diberlakukannya suatu pembatasan pengumpulan data untuk aktifasi dan individualisasi client DRM.

Database architecture and management, dengan maksud bahwa suatu system database harrus dapat menyediakan lapisan/layer suatu teknologi privacy data. Suatu data dapat disegmentasi menurut kelompok-kelompok yang berbeda sesuai dengan kesamaan yang yang dimiliki, hal tersebut dinamakan prinsip split database dan pemisahan tugas Sebagai contoh, bagian akunting perusahaan memerlukan daftar nama konsumen dan alamat pembayaran dan bagian pelayanan konsumen memerlukan bukti pembayaran untuk memeriksa validitas suatu garansi. Sistem DRM harus dapat menyediakan pseudomisasi yang mudah yang dapat digunakan untuk database kunci.

Client-side data aggregation, dengan maksud bahwa bagian ini memudahkan penggunaan teknologi skala rendah untuk privacy yang digunakan untuk pelayanan berbasis statistic. Singkatnya, pada client-side data aggregation,terjadi suatu pengelompokoan dan pemprofilan penggunaan suatu konten digital oleh pengguna. Misal, pengguna A, pada minggu lalu telah mengakses 15 album musik pop, 8 musik cadas, 7 musik dangdut dan memutar 30 jam musik dangdut dan 5 jam keroncong.

Prinsip sederhan PE lainnya, diantaranya *Transferring processed data, Competition of services, Purpose disclosure.*

KESIMPULAN

Dari sekian penjelasan sebelumnya, rangkuman dari itu semua bahwa untuk membuat usaha PE berjalan efektif, adalah penting untuk mengerti arahan (visi dan misi) bisnis dari sekian banyak pihak-pihak yang berpartisipasi dalam bisnis itu sendiri. Arahan yang salah suatu usaha privacy mempersulit improfisasi privacy ke level yang lebih baik.
Misalkan, jika suatu pihak/perusahaan menggunakan datamining sebagai sumber utama pemodelan bisnisnya, maka perusahaan tersebut akan menolak terhadap segala pembatasan dalam praktek penumpulan data/informasi.

Seiring dengan kemajuan teknologi baik perangkat keras maupun lunak di era distribusi berbasis Internet,DRM adalah suatu konsep yang diperlukan untuk melengkapi transaksi komersial dan menjamin hak-hak stakeholder terpenuhi atau menutupi celah yang tidak dapat ditutupi oleh kryptograpi dalam perlindungan hak suatu konten digital. Namun DRM sendiri memerlukan suatu pendekatan, metode dan teknik tertentu dalam melaksanakan tugas emberikan perlindungan atas hak-hak stakeholder. Privacy engineering (PE) merupakan salah satu pendekatan agar DRM dapat bekerja secara maksimal.

DAFTAR PUSTAKA

[1] Organisation for Economic Cooperation and Development. Guidelines on the protection of privacy and transborder flows of personal data, September 1980. http://www.oecd.org/

[2] FTC advisory committee on online access and security: Final report, May 2000. http://www.ftc.gov/acoas/

[3] A non-commercial list of companies currently involved in Digital Rights Management. http://www.digital-rightsmanagement-review.com/