http://www.againsttcpa.com/what-is-tcpa.html

http://www.amazon.de/exec/obidos/ASIN/3832308857/againsttcpa-21
Unter Kontrolle | Gerald Reischl | 202 Seiten

Nicht zuletzt aufgrund der Terroranschläge in den USA ist die Diskussion um nationale Sicherheitsmaßnahmen neu entbrannt. Unter dem Deckmantel der Terrorbekämpfung sollen nun staatliche Überwachungssysteme installiert werden, mit denen auch unbescholtene Bürger und Unternehmen kontrolliert werden! Telefonate können in Zukunft problemlos abgehört und Geldflüsse länderübergreifend verfolgt und abgeglichen werden. Das Internet soll ständig mit Scannern überwacht und der gesamte e-Mail-Verkehr nach Stichworten überprüft werden. Video-, Webkameras und auch Satelliten werden jeden einzelnen von uns auf Schritt und Tritt verfolgen, Software im Hintergrund wird die Bilder analysieren und Persönlichkeitsprofile erstellen. Kein Unternehmen und kein Bürger wird sich dieser totalen Kontrolle entziehen können
Nicht zuletzt aufgrund der Terroranschläge in den USA ist die Diskussion um nationale Sicherheitsmaßnahmen neu entbrannt. Unter dem Deckmantel der Terrorbekämpfung sollen nun staatliche Überwachungssysteme installiert werden, mit denen auch unbescholtene Bürger und Unternehmen kontrolliert werden!

http://www.amazon.de/%C3%9Cberwachungsmafia-lukrative-Gesch%C3%A4ft-unseren-Daten/dp/customer-reviews/3453620100/ref=dp_top_cm_cr_acr_txt?ie=UTF8&showViewpoints=1&customer-reviews.start=1#customerReviews
Die Überwachungsmafia. Das lukrative Geschäft mit unseren Daten (Broschiert)
Wenn wir unsere Privatsphäre schützen wollen, müssen wir uns auf unsere Bürgerrechte berufen und dafür kämpfen. RFID und andere Überwachungstechnologien machen es außerdem heute schon möglich jeden gezielt auf Schritt und Tritt zu überwachen.

Hier wollen wir das Ganze etwas entwirren und uns auf die Kernpunkte konzentrieren. Auf den ersten Blick ist es nämlich meist unmöglich, dass Geflecht aus Technologien, Konzernen und Gesetzen, im Ganzen zu erfassen.

Die Technologie:
TCPA steht für Trusted Computing Platform Alliance (Vertrauenswürdige Computerplattform Allianz). Bei der Technologie sprechen wir also von der TCP (Der Vertrauenswüdigen Computerplatform). Diese sieht vor, dass anfangs alle Computer mit einem TPM (Trusted Platform Module), auch bekannt als Fritz-Chip, ausgestattet werden. In späteren Entwicklungsstufen werden dessen Funktionen direkt in CPUs, Grafikkarten, Festplatten, Soundkarten, Bios usw. integriert. Dies stellt dann sicher, dass der Computer sich jederzeit in einem TCPA-Konformen Zustand befindet und dies überwacht. Präzise ausgedrückt heißt das: Auf der untersten Ebene befindet sich die Hardware, darüber TCPA, und erst danach kommt der User. Die gesamte Kommunikation arbeitet mit einer 2048Bit starken Verschlüsselung, also sicher genug, um das Entschlüsseln in Echtzeit auch auf längere Sicht zu verhindern. Dies dient dazu, sicherzustellen, dass die TCPA jegliche ungewollte Software & Hardware unterbinden kann. Daraus resultierend wird man Software und Hardware, welche nicht von diesem Konsortium abgesegnet (Zertifiziert) wurde, nicht einsetzen können. Und um diese zertifizieren zu lassen, wird man voraussichtlich, zumindest für Privatpersonen bzw. kleine & mittelständische Unternehmen, horrende Summen bezahlen müssen. Demzufolge würde man OpenSource praktisch zum Tode verurteilen, da eine Software ohne TCPA-Lizenz einfach nicht lauffähig wäre. Auf Kurz oder Lang würden nur die großen Softwareunternehmen überleben und den Markt nach belieben beherrschen können.
Wer jetzt meint, man könne dieses System doch sicher umgehen/entfernen, dürfte sich täuschen. Erstens gab es bisher noch nie eine solch in die Hardware integrierte Sicherheitstechnologie, zweitens waren es bisher immer Offline-Systeme. Bei TCP werden die Rechte zentral von der TCPA (USA?) verwaltet. Und sobald das System eine Manipulation bemerkt, wird dies gemeldet werden. Was dies strafrechtlich zur Folge haben könnte, erläutern wir unter "Die Gesetzesentwürfe". Das somit auch Systeme, die aus gutem Grund (Geschäftsdaten) nicht ans Netz sollen, zumindest zeitweise zum Schlüsselabgleich, auch online sein müssten, wäre da noch ein weiteres Übel.

Die Unternehmen:
Gegründet wurde die TCPA 1999 von Compaq, HP, IBM, Intel und Microsoft. Bis heute gehören ihr jedoch schon 200 Unternehmen an. Darunter finden sich Adobe, AMD, Fujitsu-Siemens, Gateway, Motorola, Samsung, Toshiba und viele weitere bekannte Unternehmen. IBM liefert schon die ersten Desktop-PC und Notebooks mit integriertem TPM aus.

Die Gesetzesentwürfe:
In den USA gibt es einen Gesetzesentwurf, den so genannten CBDPTA (Consumer Broadband and Digital Television Promotion Act). Vormals war dieser bekannt als SSSCA (Security Systems Standards and Certification Act). Die neue Bezeichnung liest sich bei weitem harmloser. Scheinbar machte es die erste Bezeichnung zu einfach, den Zweck des Gesetzesentwurfs zu verstehen.
Dieser sieht vor, sichere (also TCPA konforme) Geräte gesetzlich vorzuschreiben. Systeme welche diesem Gesetz nicht entsprechen dürften in den USA dann weder verkauft noch gekauft werden. Zuwiderhandlungen würden mit bis zu 5 Jahren Gefängnis und bis zu $500.000 Geldstrafe bestraft. Selbiges würde für die Entwicklung von "offener" Software gelten. Offen in dem Sinne, dass sie auf nicht TCP-Systemen lauffähig wäre.
Auch wenn dieses Gesetz selbstverständlich nur in den USA rechtskräftig wäre, hätte dieses katastrophale Auswirkungen für den Rest der Welt. Da US Unternehmen keine "unsichere" Software mehr entwickeln dürften, müssten andere entweder mit auf den TCP-Zug aufspringen, womit sie die Kontrolle über sich an die TCPA (USA?) abgeben würde, oder aber vollends auf Software von US-Unternehmen verzichten. Kein Windows, Solaris, MacOS, Photoshop, Winamp oder kurz gesagt, der größte Teil aller auf dieser Welt eingesetzten Software wäre nicht mehr einsetzbar.

Die Konsequenzen:
Damit sich das Ausmaß jeder für sich selbst und seine eigene Situation ausmalen kann, haben wir diesen Abschnitt sehr generell gehalten. Es sollte aber ein leichtes sein, anhand dieser Punkte die für sich selbst daraus resultierenden Einschränkungen zu bestimmen.

? Die informelle Selbstbestimmung ist nicht mehr existent, man kann keine Daten mehr nach eigenem Willen speichern, kopieren, erstellen, programmieren, ... Sowohl für private als auch für Firmen
? Der freie Zugang zum EDV/Software Markt ist für Nicht-Konzerne völlig unterbunden, der Markt wie wir ihn heute kennen völlig zerstört
? Einschränkung des Eigentumsrechts an gekaufter Hardware
? Die Meinungsfreiheit und das freie Wort im Internet sind endgültig beseitigt
? Das Recht auf Privatsphäre bei der EDV Nutzung ist Geschichte
? Die Nationale Unhabhängigkeit der einzelnen Staaten ist nun völlig in der Hand der Amerikaner
? Die Welt bricht digital in zwei (Staaten die sich gegen TCP aussprechen)
Wem jetzt nicht die Alarmglocken bis zum jüngsten Gericht läuten, kann getrost darauf verzichten Ross Andersons ausführliche FAQ zu lesen.

Quellen:
Lucky Greens Defcon X slides (PDF, englisch)
Ross Andersons TCPA/Palladdium-FAQ (Deutscher link oben)
Heise Newsticker: Totale Copyright-Kontroller per US-Gesetz
Experten warnen vor massiven Problemen bei TCPA und Palladium