BLOQUEO (LOCKDOWN)[1]

La guerra futura en la computación de uso general.

Por Cory Doctorow.[2]

Este artículo está basado en una presentación en el Chaos Computer Congress en Berlín, en diciembre de 2011.

Las computadoras de uso general son asombrosas. Son tan asombrosas que nuestra sociedad todavía lucha a brazo partido para saber para qué son, cómo adaptarse a ellas, y cómo hacerles frente. Esto nos lleva a algo sobre lo que debes estar harto de leer: el *copyright*.

Pero ten paciencia, porque esto es sobre algo más importante. La estructura de las guerras de copyright nos pone en la pista de una lucha por llegar sobre el destino de la propia computadora de uso general.

Al principio, todos teníamos software[3] empaquetado, y todos teníamos *sneakernet*[4]. Teníamos discos flexibles en envases herméticos, en cajas de cartón, colgadas de ganchos en las tiendas, y se vendían como los dulces o las revistas. Eran eminentemente susceptibles a la duplicación, se podían reproducir rápida y abundantemente, y eso disgustaba a la gente que hacía y vendía software.

Por eso aparece la *gestión de derechos digitales*[5] en su forma más primitiva: llamémosle DRM 0.96. Introdujeron indicios físicos que el software

---

[1] Traducción de Miguel Andúgar Miñarro.

[2] Para más información sobre el autor, puede consultar: http://en.wikipedia.org/wiki/Cory_Doctorow (N. del T.)

[3] Se conoce como *software* al equipamiento lógico o soporte lógico de un sistema informático; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware. (WIKIPEDIA) (N. del T.)

[4] Transferencia de información de un dispositivo a otro por medios físicos, como un lápiz de memoria o un cd. (Nota del T.)

[5] *Digital Rights Management,* DRM por sus siglas en inglés. (N. del T.)

comprobaba –daños deliberados, *dongles*[6], sectores ocultos- y protocolos desafío-respuesta que requerían estar en posesión de grandes y pesados manuales que eran complicados de reproducir.

Esto falló por dos razones. Primero, porque eran comercialmente impopulares, ya que reducían la utilidad del software para los dueños legítimos. Los compradores honestos se resintieron de la escasa funcionalidad de sus copias, odiaban la escasez de puertos libres, perdidos por los *dongles*, y se irritaban ante la inconveniencia de tener que cargar con grandes manuales cuando querían ejecutar su software. Segundo, eso no paró a los piratas, que podían fácilmente parchear el software y saltarse la autenticación. La gente que usaba el software sin pagar por él no se veía perjudicada.

Típicamente, la forma en la que esto sucedía era que un programador, en posesión de la tecnología y la experiencia equivalente a la del propio vendedor del software, usaba ingeniería inversa y hacía circular versiones *craqueadas*[7]. Aunque esto pudiera parecer tarea para expertos, no lo era realmente. Averiguar qué está haciendo el programa cabezota y saltarse los defectos de los soportes eran competencias básicas para los informáticos, especialmente en una era de frágiles discos flexibles y los primeros días del desarrollo de software. Las estrategias anti copia se volvieron más frágiles mientras las redes se extendían; cuando tuvimos boletines, servicios en línea, grupos de noticias USENET y listas de correo, la pericia de la gente que descubría cómo derrotar esos sistemas de autenticación podía ser empaquetada en software en forma de pequeños *cracks*. Mientras la capacidad de la red crecía, las imágenes de discos craqueadas o los mismos ejecutables podían distribuirse fácilmente.

Esto nos proporcionó el DRM 1.0. En 1996, quedó claro para todo el mundo en los pasillos del poder que algo importante estaba a punto de ocurrir. Estábamos a punto de tener una economía de la información, sea lo que sea que signifique esto. Asumieron que consistía en una economía donde comprábamos y vendíamos información. Las tecnologías de la información mejoran la eficiencia, ¡así que podéis imaginaros los mercados que una economía de la

[6] Mecanismo físico diseñado para asegurar que una pieza de software es copiada o utilizada solo por su dueño legítimo. (N. del T.)

[7] La finalidad del crack informático es la de romper las protecciones o impedimentos, y modificar las propiedades del software sin autorización de su dueño legal. (N. del T.)

información tendría! Podrías comprar un libro por un día, podrías vender el derecho a ver una película por un euro, y podrías alquilar el botón de pausa por un penique por segundo. Podrías ver películas a un precio en un país, a otro precio en otro, etc. Las fantasías de esos días eran como una aburrida adaptación fantástica del libro de los números del Viejo Testamento, una tediosa enumeración de cada permutación de cosas que la gente hace con la información –y lo que se puede cobrar por cada una.

Desafortunadamente para ellos, nada de esto sería posible a menos que pudiesen controlar cómo la gente usa sus computadoras y los archivos que transfieren a ellas. Después de todo, era fácil hablar acerca de vender a alguien una canción para descargar en su reproductor de MP3, pero no tan fácil hablar sobre el derecho de mover música del reproductor a otro mecanismo. ¿Pero cómo demonios podrías impedírselo una vez que le has dado el archivo? Para poder hacerlo, tienes que descubrir cómo impedir que las computadoras ejecuten determinados programas e inspeccionar ciertos archivos y procesos. Por ejemplo, puedes encriptar el archivo, y entonces obligar a que el usuario ejecute un programa que solo desbloquea el archivo bajo ciertas circunstancias.

Pero, como se dice en Internet, *ahora tienes dos problemas*.

Debes también impedir que el usuario guarde el archivo mientras éste permanezca desencriptado –lo cual debe ocurrir eventualmente- y debes impedir que el usuario averigüe donde almacena sus claves el programa desbloqueador, permitiéndoles desencriptar el medio y enterrar la estúpida aplicación de reproducción por completo.

Ahora tienes *tres* problemas: debes impedir a los usuarios que descubran el truco compartirlo con otros usuarios. Ahora tienes *cuatro* problemas, porque debes impedir a los usuarios que hallaron cómo extraer los secretos de los programas de desbloqueo que compartan su manera de hacerlo. Y ahora tienes *cinco* problemas, ¡porque debes impedir que los usuarios que extrajeron esos secretos les digan a otros donde están esos secretos!

Eso son un montón de problemas. Pero en 1996, tuvimos una solución. Aparece el tratado de Copyright de la OMPI[8], aprobado por la Organización Mundial de la Propiedad Intelectual de Naciones Unidas. Se crearon leyes que hicieron ilegal extraer secretos de programas desbloqueadores, y se crearon leyes que hicieron ilegal extraer *media* (como canciones y películas) de los programas de desbloqueo mientras éstos estaban ejecutándose. Se crearon leyes que hicieron ilegal decirle a la gente cómo extraer secretos de programas de desbloqueo, y se crearon leyes que hacían ilegal hospedar trabajos con *copyright* o los secretos. También establecía un proceso útil y optimizado que permitía quitar elementos de Internet sin tener que lidiar con abogados, jueces y toda esa basura.

Y con ello, la copia ilegal acabó para siempre, la economía de la información floreció en forma de bella flor que trajo prosperidad en todo el mundo; como dicen en los portaaviones, "Misión cumplida".

No es así como acaba la historia, por supuesto, porque casi cualquiera que comprendía las computadoras y las redes comprendió que esas leyes podían generar más problemas de los que resolvían. Después de todo, esas leyes hacían ilegal mirar dentro de tu computadora cuando estaba ejecutando determinados programas. Hicieron ilegal el decirle a la gente lo que encontrabas cuando mirabas en tu computadora, e hicieron fácil censurar material en Internet sin tener que probar que algo malo había ocurrido.

En poco tiempo, hicieron demandas irreales a la realidad y la realidad no las cumplió. Copiar simplemente se hizo más *fácil* tras la aprobación de esas leyes -copiar solo se *hará* más fácil. Nunca será más difícil que ahora. Vuestros nietos os pedirán: "Cuéntalo otra vez, abuelo, aquello de cuando era difícil copiar cosas en 2012, cuando no podías conseguir un disco del tamaño de una uña que pudiese almacenar todas las canciones que existen, todas las películas, todas las palabras, todas las fotografías tomadas, todo, y transferirlo en un periodo tan corto de tiempo que ni percibes que lo estás haciendo".

La realidad se impone. Como la rima de la niñera que se traga una araña para cazar una mosca, y tiene que tragar un pájaro para cazar a la araña, y un gato para cazar al pájaro, así son estas regulaciones, que tienen cierto atractivo

[8] Organización Mundial de la Propiedad Intelectual. (N. del T.)

general, pero son desastrosas en su implementación. Cada regulación conlleva una nueva, dirigida a solventar sus fallos.

Es tentador concluir aquí y afirmar que el problema es que los legisladores son o estúpidos o malvados, o quizás malvadamente estúpidos. Pero éste no es un buen camino, porque es fundamentalmente una rendición; sugiere que nuestros problemas no pueden ser resueltos mientras la estupidez y la maldad estén presentes en los pasillos del poder, lo cual implica que nunca serán resueltos. Pero yo tengo otra teoría acerca de lo que ha sucedido.

No es que los reguladores no comprendan la tecnología de la información, porque sería posible no ser un experto y hacer aún así una buena ley. Diputados, senadores y demás son elegidos para representar distritos y gente, no disciplinas ni temáticas. No tenemos un miembro del Parlamento para la bioquímica, y no tenemos un senador para el estado global de la planificación urbana. Y, aún así, estas personas que son expertos en política, no en disciplinas técnicas, todavía se las apañan para hacer buenas normas que tienen sentido. Esto sucede porque el gobierno se apoya en la heurística: reglas de oro sobre cómo equilibrar la participación de los expertos desde distintos enfoques sobre un problema.

Desafortunadamente, la tecnología de la información confunde esta heurística –la destruye completamente- en un aspecto importante.

Las pruebas necesarias para comprobar si una norma es adecuada para un propósito son: primero, si funcionará, y segundo, si tendrá en su ejecución -tanto si funciona como si no- *efectos en todo lo demás*. Si yo quiero que el Parlamento, el Congreso, o la UE regulen el uso de la rueda, es improbable que triunfe. Si señalase que los ladrones de bancos escapan siempre en vehículos con ruedas, y preguntase, "¿Podemos hacer algo sobre esto?", la respuesta sería "No". Y es así porque no sabemos cómo hacer una rueda que sea útil para los usos legítimos de la misma, pero inútil para los tipos malos. Todos podemos apreciar que los beneficios generales de las ruedas son tan importantes que sería una tontería arriesgarse a cambiarlas en un estúpido intento de parar a los ladrones de bancos. Incluso si hubiera una epidemia de robos de bancos –incluso si la sociedad estuviera al borde del colapso por los robos de bancos- nadie pensaría que las ruedas fuesen el tema apropiado para empezar a resolver nuestros problemas.

En cualquier caso, si yo fuese a esa misma cámara para decir que tengo pruebas irrefutables de que los teléfonos manos-libres convierten a los coches en artefactos peligrosos, y solicitase una ley prohibiendo dichos teléfonos en los coches, el regulador podría decir "Sí, lo capto, podríamos hacerlo".

Podríamos estar en desacuerdo sobre si es o no una buena idea, o si mis pruebas tienen o no sentido, pero pocos de nosotros diríamos que una vez que retiras de los coches los dispositivos de manos libres, los coches *dejan de ser coches*.

Comprendemos que los coches siguen siendo coches incluso si les quitamos algunas de sus características. Los coches tienen un propósito específico, al menos en comparación con las ruedas, y los manos libres añaden una utilidad a una tecnología previamente especializada. Hay una heurística para esto: las tecnologías de propósito específico son complejas, y puedes extraer características de las mismas sin cometer un acto de violencia contra su utilidad subyacente.

Esta regla de oro sirve bien al regulador, en general, pero se presenta inefectiva para la computadora de propósito general y la red de propósito general –el PC e Internet. Si piensas en el *software* como una característica, una computadora que ejecuta una hoja de cálculo tiene la funcionalidad de una hoja de cálculo, y una que ejecute World Of Warcraft[9] tiene una utilidad MMORPG[10]. La heurística te llevaría a pensar que una computadora incapaz de ejecutar hojas de cálculo o juegos no sería peor para la informática que la prohibición de los teléfonos para coches lo sería para el mundo del automóvil.

Y, si piensas que los protocolos y los sitios web son características de la red, entonces diciendo "arregla Internet para que no funcione Bittorrent[11]", o "arregla Internet para que thepiratebay.org[12] no resuelva", suena muy parecido a "cambia el tono de la señal de ocupado", o "saca a esa pizzería de la esquina fuera de la red telefónica", y no como un ataque a los principios fundamentales de las redes.

[9] Famoso videojuego de rol multijugador en línea. (N. del T.)
[10] Videojuego de rol multijugador masivo en línea. (N. del T.)
[11] Protocolo descentralizado de intercambio de archivos. (N. del T.)
[12] Buscador de archivos para su descarga a través de redes descentralizadas. (N. del T.)

La regla de oro funciona para coches, para casas, y para cualquier otra área esencial de la regulación de lo tecnológico. No darse cuenta de que falla para Internet no te hace malvado, ni te hace ignorante. Te hace parte de una vasta mayoría, para la que ideas como la completitud de Turing o el principio *end-to-end* no tienen sentido.

Así, nuestros reguladores se lanzan, alegremente aprueban esas leyes, y se convierten en parte de la realidad de nuestro mundo tecnológico. Ellos son, de repente, los números que no se nos permite escribir en Internet, los programas que no estamos autorizados a publicar, y todo lo que cuesta hacer desaparecer de Internet material legítimo, es la mera acusación de violación de propiedad intelectual. Fallan a la hora de alcanzar la meta de la regulación, porque no impiden que la gente viole las leyes de copyright, pero asemeja superficialmente a la *satisfacción* de los derechos de autor –satisface el silogismo de seguridad: "algo debe hacerse, estoy haciendo algo, algo se ha hecho". Como resultado, cualquier fallo que surja puede ser atribuido a la idea de que la regulación no ha ido lo bastante lejos, en lugar de que la idea estaba equivocada desde el principio.

Este tipo de parecido superficial y divergencia subyacente ocurre en otros contextos de ingeniería. Tengo un amigo, que fue una vez ejecutivo *senior* en una gran compañía de productos envasados, que me contó lo que ocurría cuando el departamento de marketing le decía a los ingenieros que se les había ocurrido una gran idea para un detergente: ¡a partir de este momento, vamos a hacer detergente que haga que tus ropas sean más nuevas cada vez que las lavas!

Después de que los ingenieros intentaran sin éxito transmitir el concepto de entropía al departamento de marketing, llegaron con otra solución: desarrollarían un detergente que usaría enzimas para atacar los cabos sueltos de las fibras rotas que hacen que tu ropa parezca vieja. Usarlo literalmente provocaría que tus ropas *se disolvieran en la lavadora*.

Esto es, no hace falta decirlo, lo contrario de hacer las ropas más nuevas. En su lugar, las envejecerías artificialmente cada vez que las lavaras, y, como usuario, cuanto más usases la "solución", más drásticas serían las medidas necesarias para mantener tus ropas nuevas. Eventualmente, tendrías que comprar ropa nueva porque las viejas se destruirían.

Hoy tenemos departamentos de marketing que dicen cosas como "no necesitamos computadoras, necesitamos aparatos. Hazme una computadora que no ejecute cualquier programa, solo un programa que haga esta tarea especializada, como reproducir audio en *streaming*, o enrutar paquetes, o ejecutar juegos de Xbox, y asegúrate que no ejecute programas que no he autorizado y que podrían reducir nuestros beneficios."

A primera vista, parece una idea razonable: un programa que haga una tarea especializada. Después de todo, podemos poner un motor eléctrico en una licuadora, y podemos instalar un motor en un lavavajillas, y no nos preocupamos si se puede ejecutar un programa de lavado en una licuadora. Pero eso no es lo que hacemos cuando convertimos una computadora en un dispositivo. No estamos haciendo una computadora que solo ejecuta la aplicación "dispositivo"; estamos usando una computadora que puede ejecutar cualquier programa, entonces usamos una combinación de rootkits[13], software espía, y firmas de código para evitar que el usuario sepa qué procesos se están ejecutando, evitar que pueda instalar su propio software, y evitar que finalice procesos indeseables. En otras palabras, un dispositivo no es una computadora despojada; es una computadora completamente funcional con spyware de fábrica.

No sabemos cómo construir una computadora de uso general que sea capaz de ejecutar cualquier programa excepto alguno que no nos guste, que esté prohibido por ley, o que nos haga perder dinero. Lo más aproximado que tenemos es una computadora con software espía: una computadora en la cual terceras personas establecen políticas sin conocimiento del usuario, o por encima de la objeción del propietario de la computadora. La gestión de derechos digitales siempre converge a malware[14].

En un famoso incidente –un regalo para la gente que comparte esta hipótesis- Sony cargó instaladores encubiertos de rootkits en 6 millones de CDs de audio, que secretamente ejecutaban programas que vigilaban buscando intentos de leer los archivos de sonido en los CDs, y los detenían. También ocultaban la existencia del rootkit obligando al núcleo del sistema operativo a mentir acerca de qué procesos estaba ejecutando, y qué archivos estaban

[13] Programa que accede a información de una computadora ocultando su presencia al usuario o propietario. (N. del T.)

[14] Software malintencionado. (N. del T.)

presentes en el disco. Pero no es el único ejemplo. La Nintendo 3DS oportunistamente actualiza su *firmware*[15] y hace una prueba de integridad para asegurarse de que no has alterado el anterior *firmware* de ninguna manera. Si detecta signos de manipulación, se convierte a sí misma en un ladrillo.

Los activistas de derechos humanos han dado la alarma respecto a U-EFI, el nuevo sistema de arranque de PC, que limita tu computadora para que ésta solo ejecute sistemas operativos "firmados", señalando que los gobiernos represores probablemente retengan las firmas de los sistemas operativos a menos que éstos permitan operaciones de vigilancia encubierta.

En lo que a la red concierne, los intentos de hacer una red que no pueda ser usada para la violación del *copyright* siempre convergen con las medidas de vigilancia que conocemos de gobiernos represores. Consideren SOPA, la Ley para Detener la Piratería En Línea, que prohíbe herramientas inocuas como DNSSec –una *suite* de seguridad que autentifica nombres de dominio- porque podría ser usada para superar medidas de bloqueo de DNS. Bloquea Tor, una herramienta de anonimato en línea patrocinada por el U. S. Naval Laboratory y usada por disidentes de regímenes opresores, porque puede ser usada para evitar medidas de bloqueo de IPs[16].

De hecho, la Motion Picture Association of America, uno de los proponentes de SOPA, hizo circular un informe citando investigaciones que afirmaban que SOPA podría funcionar *porque* usaba las mismas medidas que se usan en Siria, China y Uzbekistán. Argumentaba que puesto que esas medidas son efectivas en esos países, ¡funcionarían también en América!

Podría parecer que SOPA es el fin de juego en una larga lucha sobre copyright e Internet, y podría parecer que si derrotamos a SOPA, iremos por buen camino para asegurar la libertad de nuestros PCs y redes. Pero como dije al principio de esta charla, esto *no es* sobre copyright.

Las guerras de copyright son solo la versión beta de una larga guerra en la computación aún por llegar. La industria del entretenimiento es solo la primera beligerante en tomar las armas, y tendemos a pensar en ellos como

[15] Instrucciones de propósitos específicos, vinculadas a la propia electrónica física del dispositivo. (N. del T.)

[16] El número IP sirve para identificar una computadora conectada a una red, e indirectamente el lugar desde el que está conectada y la identidad de su propietario. (N. del T.)

particularmente exitosos. Después de todo, ahí está SOPA, balanceándose en el límite de la aprobación, preparada para romper Internet a un nivel fundamental –todo en el nombre de preservar la música de los 40 principales, los shows de telerrealidad, y las películas de Ashton Kutcher.

Pero la realidad es que la legislación sobre *copyright* llega tan lejos como lo hace porque no es tomada en serio por los políticos. Esta es la razón por la que, por un lado, en Canadá se han presentado legislatura tras legislatura, horribles leyes sobre *copyright*, pero por otro, legislatura tras legislatura han fracasado en su intento. Esta es la razón por la fueron aplazadas las urgentes sesiones sobre la SOPA, una ley compuesta de *pura estupidez* y unida molécula a molécula en una especie de "Estupidina 250" normalmente solo encontrada en el corazón de estrellas recién nacidas: para que los legisladores pudiesen dedicarse a un debate nacional sobre un tema importante, el seguro de desempleo.

Esa es la razón por la que se engaña una y otra vez a la Organización Mundial de Propiedad Intelectual promulgando locas y analfabetas propuestas sobre copyright: porque cuando las naciones del mundo envían sus misiones de la O.N.U. a Ginebra, envían a expertos en hidrología, no a expertos en copyright. Envían expertos en salud, no expertos en copyright. Envían expertos en agricultura, no expertos en copyright, porque el copyright sencillamente, no es tan importante.

El Parlamento canadiense no votó sobre sus leyes de copyright porque, de todas las cosas que Canadá necesita hacer, arreglar el copyright está muy por debajo de emergencias de salud en las reservas de las Primeras Naciones, explotar el petróleo de Alberta, interceder en resentimientos sectarios entre francófonos y anglófonos, resolver crisis de recursos en los caladeros de la nación, y otros mil asuntos. La trivialidad del copyright te dice que cuando otros sectores de la economía comienzan a manifestar intereses sobre Internet y los PCs, el copyright se mostrará como una escaramuza menor –no una guerra.

¿Por qué llegarían otros sectores a albergar rencores contra las computadoras al igual que la industria del entretenimiento? El mundo en que vivimos está *hecho* de computadoras. No tenemos coches; tenemos computadoras que nos llevan de un sitio a otro. No tenemos ya aviones; tenemos cajas Solaris voladoras unidas a montones de sistemas industriales de control.

Una impresora 3D no es un mecanismo, es un periférico, y solo funciona conectado a una computadora. Una radio no es ya un cristal: es una computadora de uso general, ejecutando software. Las quejas que surgen por las copias no autorizadas de *Snooki's Confessions of a Guidette* son triviales comparadas con las llamadas a la acción que nuestra realidad llena de computadoras pronto creará.

Consideremos la radio. La regulación de radio hasta hoy estaba basada en la idea de que las propiedades de una radio son fijadas en el momento de la fabricación, y que no pueden ser fácilmente alteradas. No puedes simplemente accionar un interruptor en tu monitor para bebés e interferir otras señales. Pero poderosas radios definidas por software (SDRs) pueden cambiar de ser un monitor para bebés a despachador de emergencias o controladoras de tráfico aéreo, simplemente cargando y ejecutando software diferente. Esta es la razón por la que la Comisión Federal de Comunicaciones (FCC) consideró qué ocurriría cuando pusiésemos SDRs a funcionar, y pidió asesoramiento sobre si debería ordenarse que todas las radios definidas por software fuesen incluidas en máquinas de "computación confiable". Últimamente, la cuestión es si todo PC debe ser bloqueado, para que sus programas puedan ser estrictamente regulados por autoridades centrales.

Incluso esto es una sombra del o que queda por llegar. Después de todo, éste ha sido el año en el que vimos el debut de archivos de código abierto para convertir rifles AR-15 en completamente automáticos. Éste fue el año del *hardware* de inversión pública [crowd-funded] de código abierto para el secuenciado genético.

Y así como la impresión en 3D generará muchas protestas triviales, habrá jueces en Sudamérica y *mullahs* en Irán que perderán la cabeza porque en sus jurisdicciones se imprimirán juguetes sexuales. La trayectoria de la impresión en 3D generará quejas reales, desde laboratorios de metanfetamina de estado sólido a cuchillos de cerámica.

No se necesita a un escritor de ciencia-ficción para comprender por qué los reguladores podrían ponerse nerviosos sobre el *firmware* modificable por el usuario de coches que se conducen solos, o limitando la interoperabilidad para los controladores de aviación, o el tipo de cosa que podrías hacer con

ensambladores y secuenciadores biológicos. Imagina lo que ocurrirá el día que Monsanto determine que es realmente importante asegurarse que las computadoras no pueden ejecutar programas que permitan que periféricos especializados fabriquen organismos que *literalmente* se coman tu almuerzo.

Independientemente de que estos sean problemas reales o temores histéricos, son, en cualquier caso, la moneda política de lobbies y grupos de interés con mucha más influencia que Hollywood y el gran contenido. Todos ellos llegarán a la misma conclusión: "¿No puedes hacer una computadora de uso general que ejecute todos los programas, excepto los que nos asustan y nos enfadan? ¿No puedes hacernos un Internet que transmita cualquier mensaje sobre cualquier protocolo entre dos puntos, excepto si nos molesta?"

Habrá programas que se ejecuten en computadoras de uso general, y periféricos, que incluso me enloquecerán incluso a mí. Así que puedo creer que la gente que aboga por limitar las computadoras de uso general encontrará una audiencia receptiva. Pero, como vemos con las guerras del copyright, prohibir ciertas instrucciones, protocolos o mensajes será completamente ineficaz como medida de prevención y remedio. Como vemos en las guerras de copyright, todos los intentos de controlar los PCs convergerán en *rootkits*, y todos los intentos de controlar Internet convergerán en vigilancia y censura. Este asunto importa porque hemos pasado la última década enviando a nuestros mejores jugadores a luchar con lo que pensábamos que era el jefe final al final del juego, pero al final ha sido un guardián de fin de nivel. Lo que está en juego va a ser algo más importante.

Como miembro de la generación Walkman, he hecho las paces con el hecho de que necesitaré ayuda para la audición antes de morir. No será un audífono, sin embargo; será realmente una computadora. Así que cuando me meta en un coche –una computadora en la que meto mi cuerpo- con mi audífono –una computadora que meto en mi cuerpo- quiero saber que esas tecnologías no están diseñadas para guardarme secretos, o impedir que finalice procesos en dichos dispositivos que trabajan contra mis intereses.

El año pasado, la Lower Merion School District, en un suburbio de clase media de Filadelfia, se encontró en graves problemas. Fue cogida distribuyendo a sus estudiantes portátiles pirateados que permitían la vigilancia remota

mediante la cámara del portátil y la conexión a Internet. Ellos fotografiaban a los estudiantes miles de veces, en casa y en la escuela, despiertos y dormidos, vestidos y desnudos. Mientras, la última generación de tecnología de interceptación legal puede secretamente operar cámaras, micrófonos, y receptores GPS en PCs, *tablets*, y dispositivos móviles.

No hemos perdido todavía, pero tenemos que ganar la guerra del copyright primero si queremos mantener Internet y los PCs libres y abiertos. La libertad en el futuro requerirá de nosotros tener la capacidad de monitorizar nuestros dispositivos y establecer políticas significativas para ellos; examinar y finalizar los procesos de software que ejecutan; y mantenerlos como honestos servidores de nuestra voluntad, no como traidores y espías trabajando para criminales, matones, y obsesionados con el control.