Manifiesto Cypherpunk

por Eric Hughes

La privacidad es necesaria para una sociedad abierta en la era electrónica.
La privacidad no es secretismo. Un asunto privado es algo que no quieres que lo sepa el mundo entero; un asunto secreto es algo que no quieres que lo sepa nadie. La privacidad es el poder de revelarse selectivamente al mundo.

Si dos partes realizan una transacción, cada una tiene un recuerdo de su interacción. Cada parte puede hablar sobre su propia memoria, ¿quién puede impedirlo? Podrías aprobar leyes contra ello, pero la libertad de expresión, aún más que la privacidad, es fundamental en una sociedad abierta; no buscamos restringirla en absoluto. Si muchos hablan juntos en el mismo foro, cada uno puede comunicarse a todos los demás y agregar conocimiento sobre individuos y otros participantes. El poder de las comunicaciones electrónicas permite ese discurso colectivo, y no desaparecerá solo porque queramos.

Ya que deseamos privacidad, debemos asegurarnos de que cada parte en una transacción conozca únicamente lo que resulta estrictamente necesario para esa transacción. Ya que cualquier información puede transmitirse, debemos garantizar revelar lo menos posible. En la mayoría de casos, la identidad personal no es relevante. Cuando compras una revista en una tienda y pagas en efectivo, no hace falta que sepan quién eres. Cuando pido a mi proveedor de correo electrónico que envíe y reciba mensajes, no debe saber con quién hablo, qué digo o qué me dicen los demás; solo necesita saber cómo hacer llegar el mensaje y cuánto debo pagar. Cuando la identidad se revela por el mecanismo subyacente de la transacción, no tengo privacidad. No puedo revelar selectivamente; tengo que revelarme siempre.

Por tanto, la privacidad en una sociedad abierta exige sistemas de transacciones anónimas. Hasta ahora, el efectivo ha sido el sistema principal. Un sistema anónimo no es un sistema secreto. Un sistema anónimo permite al individuo revelar su identidad cuando desea y solo cuando lo desea; esa es la esencia de la privacidad.

La privacidad en una sociedad abierta también requiere criptografía. Si digo algo, quiero que solo las personas a las que va dirigido lo oigan. Si el contenido de mi mensaje está disponible para el mundo, no tengo privacidad. Cifrar es indicar el deseo de ser privado; cifrar con criptografía débil es indicar un deseo limitado. Además, revelar la identidad con certeza cuando el anonimato es la norma requiere firmas criptográficas.

No podemos esperar que gobiernos, corporaciones u otras grandes entidades nos otorguen privacidad por su benevolencia. Les conviene hablar de nosotros, y debemos esperar que lo hagan. Tratar de impedir su discurso es ir en contra de las realidades de la información. La información no solo quiere ser libre; anhela serlo. La información crece para llenar el espacio disponible. La Información es la hermana veloz del Rumor;

la Información es más rápida, tiene más ojos, sabe más, y entiende menos que el Rumor.

Debemos defender nuestra propia privacidad si queremos tener alguna. Debemos unirnos y crear sistemas que permitan transacciones anónimas. Las personas han defendido su privacidad durante siglos con susurros, oscuridad, sobres cerrados, puertas, apretones de manos secretos, y mensajeros. Las tecnologías del pasado no permitían una privacidad fuerte, pero las tecnologías electrónicas sí.

Nosotros, los Cypherpunks, estamos comprometidos en construir sistemas anónimos. Defendemos nuestra privacidad con criptografía, sistemas anónimos de reenvío de correo, firmas digitales y dinero electrónico.

Los cypherpunks escriben código. Sabemos que alguien debe escribir el software que defienda la privacidad, y como no podemos obtenerla si no lo hacemos, nosotros lo escribiremos. Publicamos nuestro código para que otros cypherpunks puedan practicar y experimentar con él. Nuestro código es libre y accesible para todos, en todo el mundo. No nos importa si no apruebas nuestro software. Sabemos que el software no puede ser destruido y que un sistema distribuido ampliamente no puede ser detenido.

Los cypherpunks deploran las regulaciones sobre la criptografía, porque cifrar es un acto esencialmente privado. El cifrado saca información del dominio público. Incluso las leyes contra la criptografía solo tienen alcance dentro de un país. La criptografía se extenderá inevitablemente por todo el mundo, al igual que los sistemas de transacción anónimos que posibilita.

Para que la privacidad sea generalizada, debe formar parte de un contrato social. Las personas deben fomentar e implementar estos sistemas por el bien común. La privacidad solo llega hasta donde la cooperación de las personas permita. Nosotros, los cypherpunks, buscamos tus preguntas y preocupaciones, con la esperanza de involucrarnos y no autoengañarnos. Sin embargo, no nos desviaremos de nuestro curso porque haya quienes no compartan nuestros objetivos.

Los cypherpunks están activamente comprometidos en hacer las redes más seguras para la privacidad. Continuemos juntos, sin demora.

Adelante.

Eric Hughes
hughes@soda.berkeley.edu
9 de marzo de 1993