Manifeste d'un Cypherpunk,

Eric Hughes, <hughes@soda.berkeley.edu>

La vie privée est nécessaire pour une société ouverte dans l'ère électronique. La vie privée n'est pas un secret. Une affaire privée est ce qu'un individu ne veut que le monde entier sache, mais une affaire secrète est ce qu'un individu ne veut que quiconque sache.

La vie privée est le pouvoir de se révéler sélectivement au monde. Lorsque deux partis ont une certaine forme d'échange, chacun possède ensuite un souvenir de leur interaction. Chaque parti peut parler de son propre souvenir de l' échange; comment quelqu'un pourrait-il empêcher cela? Des lois pourraient être adoptées contre cela, mais la liberté d'expression, encore plus que celle de la vie privée, est fondamentale à une société ouverte; nous ne cherchons en aucun cas à restreindre quelque expression qu'elle soit.

Si plusieurs partis dialoguent au sein d'un même forum, chaque parti peut communiquer avec tout le reste et agréger ensemble leur connaissance sur les individus et les autres partis. Le pouvoir des communications électroniques a permis une telle expression de groupe, et cela ne peut disparaître simplement parce que nous pourrions le souhaiter. Puisque nous désirons une vie privée, nous devons nous assurer lors d'un échange que chaque parti ait seulement connaissance de ce qui sera directement nécessaire à cet échange. Puisque n'importe quelle information peut être évoquée, nous devons nous assurer que nous en révélons le moins possible. Dans la plupart des cas l'identité personnelle n'est pas mise en évidence.

Quand j'achète un magazine dans une boutique et que je tends des espèces au vendeur, il est inutile de savoir qui je suis. Quand je demande à mon prestataire de services réseau d'envoyer et de recevoir des messages, mon prestataire n'a pas besoin de savoir avec qui je parle ou ce que je dis ou ce que les autres me disent; mon prestataire a seulement besoin de savoir comment il va envoyer le message et combien je lui dois pour le service fourni. Quand mon identité est révélée par le mécanisme sous-jacent de l'échange, je n'ai aucune vie privée. Je ne peux ici choisir ce que je dévoile de moi-même; je devrais toujours me révéler.

Par conséquent, la vie privée dans une société ouverte requiert des systèmes d'échanges anonymes. Jusqu'à présent, l'argent liquide a été le moyen principal d'un tel système. Un système d'échanges anonyme n'est pas un système d'échanges secret. Un système anonyme renforce le pouvoir des individus à révéler leurs identités quand ils le désirent et seulement quand ils le désirent; c'est l'essence-même de la vie privée.

La vie privée dans une société ouverte requiert également la cryptographie. Si je dis quelque chose, je veux que cela soit entendu uniquement par ceux à qui le message était destiné. Si le contenu de mon message est ouvertement disponible au monde, je n'ai pas de vie privée.

Crypter, c’est indiquer le désir d’une vie privée, et crypter avec une faible cryptographie est l’indication d’un désir faible pour une vie privée. En outre, révéler son identité avec assurance lorsque l’anonymat est par défaut requiert une signature cryptographique.

Nous ne pouvons attendre des gouvernements, des entreprises et des autres organisations majeures sans visage de nous accorder une vie privée par acte de bienveillance. C’est à leur avantage de parler de nous, et nous devrions nous attendre à ce qu’ils le fassent. Tenter de les en empêcher, c’est se battre contre les réalités du renseignement. Le renseignement ne veut pas juste être libre, il est avide de liberté. Le renseignement tend à remplir l’espace de stockage disponible. Le renseignement est le plus jeune, le plus fort des cousins de la Rumeur; le renseignement a le pied plus léger, a plus d’yeux, en connaît davantage, et comprend moins que la Rumeur.

Nous devons défendre notre vie privée par nous-mêmes si nous nous attendons à en avoir une. Nous devons nous rassembler et créer des systèmes qui nous permettent d’arriver à des échanges anonymes. Les gens ont défendu leurs propres vies privées pendant des siècles par des murmures, l’obscurité, des enveloppes, des portes fermées, des poignées de main secrètes, et des messagers. Les technologies du passé ne permettaient pas une confidentialité solide, les technologies électroniques le permettent.

Nous les Cypherpunks sommes dévoués à construire des systèmes anonymes. Nous défendons notre vie privée avec la cryptographie, avec des systèmes de renvoi anonymes, avec des signatures digitales, et avec une monnaie électronique. Les Cypherpunks écrivent du code. Nous savons que quelqu’un doit élaborer des logiciels défendant la vie privée, et puisque que nous ne pouvons avoir de vie privée à moins que nous tous en soyons pourvus, nous allons les réaliser. Nous publions notre code afin que nos semblables Cypherpunks s’entraînent et jouent avec. Notre code est libre à tous d’être utilisé, dans le monde entier. Nous ne nous en soucions guère si vous n’approuvez pas les logiciels que nous développons. Nous savons qu’un logiciel ne peut être détruit et qu’un système largement répandu ne peut être arrêté.

Les Cypherpunks déplorent les régulations sur la cryptographie, le cryptage étant fondamentalement un geste privé. En fait, le geste de crypter retire le renseignement du domaine public. Même les lois jusqu’ici contre la cryptographie atteignent seulement la frontière d’une nation et le bras de sa violence. La cryptographie va inéluctablement se répandre dans l’ensemble du globe, et avec elle les systèmes d’échanges anonymes qui la rendent possible. Pour que la confidentialité soit largement répandue faut-il qu’elle fasse partie d’un contrat social.

Le peuple doit se rassembler et déployer ensemble ces systèmes pour le bien commun. La vie privée ne peut s’étendre que grâce à la coopération entre les membres d’une société.

Nous les Cypherpunks sollicitons vos questions et vos inquiétudes et espérons que vous puissiez vous engager afin que nous ne nous fassions pas d'illusions. Nous ne nous ferons cependant pas dévier de notre course sous prétexte que certains désapprouveraient nos objectifs.

Les Cypherpunks sont activement engagés à rendre les réseaux plus sûrs pour la vie privée.

Avançons ensemble en vitesse.

En avant.

Eric Hughes
9 mars 1993

**

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy

only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Eric Hughes <hughes@soda.berkeley.edu>

9 March 1993