Journal of Information, Law and Technology

Creating A Subpoena-Proof Diary: A Technological Solution to A Legal Problem

James D Miller
Assistant Professor of Economics
Smith College
Northampton, USA
EconomicProf@yahoo.com

Lixin Gao
Associate Professor of Computer Science
Smith College
Northampton, USA

This is a **refereed** article published on: 7 November 2001

Citation: Miller, J and Gao, L, 'Creating A Subpoena-Proof Diary: A Technological Solution to A Legal Problem', Refereed article, 2001 (3) *The Journal of Information, Law and Technology (JILT)*. <http://elj.warwick.ac.uk/jilt/01-3/miller.html>

Abstract

Many high ranking government officials are afraid to keep a diary because of the possibility that it will be subpoenaed. This will undoubtedly be a great loss to future historians. This paper describes a method by which a subpoena-proof diary can be kept. The diary can be encrypted in a way such that no one, not even the author, can read it until some period of time has elapsed. In this way, the diary can be read by future historians but not by contemporary political enemies.

JIM LEHRER: *'Are you keeping a diary? Are you keeping good notes on what's happening?'*

HILLARY CLINTON: *'Heavens no! It would get subpoenaed. I can't write anything down.* [Laughing]'

Keywords:

1. Introduction

Many current and former high-ranking government officials have said that they would not keep a diary because of fear that it would be subpoenaed. Fear of a prosecutor with subpoena power is likely to prevent any future American president from keeping a reasonably complete diary unless a method can be devised to keep diaries secure. This paper suggests that authors can use computer encryption to create subpoena-proof diaries.

Computer encryption converts a plain text into a coded data file. The coded data file can be decrypted (turned back into a plain text) only by someone who has the encryption key. The encryption key is simply a number. Encryption permits a diary's author to prevent anyone from reading the diary who does not have the encryption key. However, if the author had the key, the diary would not be subpoena-proof because the subpoenaing party can demand the key, and the author would under some circumstances be legally obligated to reveal it. The only way that encryption could protect the author would be if no one, not even the author, has the encryption key. Therefore, to create a subpoena-proof diary, an author should encrypt her diary and throw away the encryption key. But then, how could the diary ever be read?

Before the author throws away the encryption key, she can perform a mathematical operation on the encryption key which produces a new number. While this new number cannot be used directly to decrypt the diary, the original key can be recovered using this new number. However, recovering the original key from this new number would take a considerable amount of time. The mathematical operation determines the amount of time it would take to recover the original encryption key from the new number. Depending on the mathematical operation used, recovering the original encryption key could take days, years or decades. During the period it would take to recover the original encryption key, the diary would be completely subpoena-proof. This method would be very useful to a president who does not want her diary to be read until after she leaves office.

The encryption scheme this paper proposes takes advantage of the continual increase in computer speeds. Because of the future expected increases in computer speeds, an encryption key that would take several years to recover today could be recovered in only a few months ten years from now.

One might think that a flaw with any subpoena-proofing method based on encryption lies in the fact that a special prosecutor or congressional committee could quickly decrypt the diary by using millions of computers coordinated via the Internet. However, under the scheme described in this paper, using multiple computers would not accelerate the recovery of the data file. The speed at which a file can be recovered is solely a function of the speed of the single fastest available computer.

Another flaw with any encryption technology is that a data file that is safe today may not be safe in the future if there is faster than expected increase in computer speeds. However, the scheme this paper proposes allows the author to strengthen the diary's security at any time during which the diary is not under subpoena.

In section I, this paper examines why diaries are not secure. The section explores why the Fourth and Fifth Amendments do not always protect a diary from subpoenas and why the logic of game theory might effectively force a politician to reveal her diary even if she is not legally required to do so. Section II explains how encryption works in general and describes an encryption scheme for keeping a subpoena-proof diary. The appendix provides a detailed technical explanation of the proposed scheme.

2. Section I. Why Diaries Are Not Secure

2.1 Fifth Amendment Protection

The Fifth Amendment to the United States Constitution provides in part that no person 'shall be compelled in any criminal case to be a witness against himself.' The United States Supreme Court used to hold that this prevented a court or prosecutor from compelling a person to release documents that she prepared. Recently, the Supreme Court ruled that the Fifth Amendment does not bar the forced release of non-personal papers. The Supreme Court has never decided whether the Fifth Amendment prevents the forced revelation of personal papers. The federal appeals courts are split on this issue.

In Boyd v. United States, a district attorney forced a business to turn over invoices that the business created. These invoices were then used as evidence against the business. The Supreme Court held that compelling an owner to produce private books or papers is the equivalent to 'compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution.' Had the Supreme Court not modified Boyd in subsequent opinions, then authors of diaries could never be compelled to reveal them.

In Fisher v. United States, the Supreme Court significantly limited the Fifth Amendment protection against the forced revelation of papers and documents. In Fisher, the Court

held that forcing an individual to produce work papers does not violate the Fifth Amendment because 'it does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought.' However, the Court explicitly wrote that their opinion does not apply to private papers, leaving open the question of whether an individual could be compelled to turn over a diary. In an concurring opinion in United States v. Doe, Justice O'Connor wrote that the Fifth Amendment provides no protection for 'private papers of any kind.' However, in a dissenting opinion in that same case, Justice Marshall wrote that he viewed the Court's ruling as not limiting the Fifth Amendment's protection for private papers. Thus, the Supreme Court has never clearly determined whether the Fifth Amendment provides protection for diaries.

The circuit courts are currently divided over whether the Fifth Amendment provides any protection for personal papers. A District Court in the District of Columbia recently held that the Fifth Amendment did not offer protection for a senator who wished to prevent a senate committee from subpoenaing his diary. Thus, it is unlikely that a federal government official would be able to use the Fifth Amendment to stop a congressional committee or a special prosecutor from obtaining her diary.

2.2 Fourth Amendment Protection

The Fourth Amendment reads in part that 'The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated.' As with the Fifth Amendment, the Fourth Amendment used to provide strong protection for individual's diaries but no longer does so.

The Supreme Court previously held that the government could seize only the instrumentalities or the fruits of crimes. The Court also used to hold that the Fourth Amendment did not allow private papers to be seized if there were mere evidence of a crime. In Warden v. Hayden, the Court reduced Fourth Amendment protections and held that there was no greater Fourth Amendment protection for evidence of crimes than for the instrumentalities or fruits of crimes. Consequently, under current constitutional doctrine, the Fourth Amendment does not protect an individual from having her diary taken if the government has a reasonable justification for believing that it contains evidence of a crime.

2.3 Effective Disclosure and Game Theory

Even if an author can be confident that her diary will never be read without her permission, she might still be reluctant to keep a diary. This is because if it is known that she is keeping a diary, not releasing it can be politically costly due to a concept in game theory known as unraveling. Unraveling can effectively force an author to release the contents of her diary.

Imagine a situation where a President is in serious political trouble. She is accused of doing something which, if true, could lead to her impeachment. Assume that it is known

that she has kept a detailed diary while in office, and that the opposition party is calling for the President to release her diary. Further imagine that the benefit or harm of the contents of the diary can be ranked on a scale from 1 to 5. The higher the number, the less harmful the information is to the President. Assume that people believe that the contents are equally likely to take on any value between 1 and 5, and that on average the contents rank a value of 3. If the President has a chance to release the diary and does not, people will reasonably believe that the contents do not rank a 4 or 5. This is because if people initially believe that the diary, on average, ranked a 3, but the President knows that it ranked higher, the President will surely release the contents of the diary. Therefore, by not releasing the contents of the diary, the President will send a signal that its contents are not higher than 3. Now that everyone knows that the diary does not rank higher than 3, people will assume that the diary is equally likely to rank a 1, 2, or 3, and that on average, people would believe that the diary would rank a 2. So, if the diary really ranks a 3, the President will surely now release its contents. If the President still refuses to release the contents of the diary, people will assume that it does not rank higher than 2. However, this would cause people to change their view about the rank of the diary. People now might assume that since the rank is not greater than 2, it is equally likely to be 1 or 2, and that on average, the contents rank a value of 1.5. If people believe that the average rank of the diary is 1.5, the President will surely release the diary if its rank is really 2. Thus, if the President does not release her diary, people will assume that it contains the worst possible information.

One can see how unraveling can force the President to reveal the contents of her diary if it does not rank a 1. If the diary's contents do in fact rank a 1 and the President does not reveal its contents, people will assume that it ranks a 1. Note that this situation is what game theorists call a stable equilibrium. If people believe that the President will release the contents of her diary unless they are ranked a 1, the President has an incentive to release the contents unless they are indeed ranked a 1. Thus, the individual's beliefs are consistent with the President's actions.

As a result, a law prohibiting a diary from being read without its author's permission might not be enough to convince a high ranking government official to keep a diary. The law would also have to forbid the author from releasing the diary while in office, but such a law would clearly be unconstitutional. The only solution to this problem is for it to be known that the President lacks the ability to release the contents of her diary.

3. Section II. The Encryption Solution

3.1 How Encryption Works

A typical encryption scheme works as follows. The plain text to be encrypted is transformed by a function that is parameterized by a key. The output of the encryption process is a coded text. A fundamental rule of cryptography is that one must assume that the encryption function is known. The encryption key is, however, typically kept secret. The person who knows the key can recover the original text by using the key and the decryption function.

Since the real secrecy is in the key, its length is a major design issue in an encryption scheme. Similar to the principle of the combination lock, if the key is two bits long, there are only 4 possibilities. The longer the key, the less likely someone can find the key by exhaustively searching all possible keys. In general, the number of possible for an n-bit key is 2^n. Therefore, one needs a long key to ensure secrecy.

3.2 A Scheme to Create a Subpoena-Proof Diary

This paper proposes that an author use a standard encryption scheme to encrypt her diary. The encryption scheme is called Data Encryption Standard (DES). DES uses mathematical functions to effectively hide the original text from someone who does not have the encryption key.

After the author has encrypted her diary, she should use a mathematical process, which is described in the appendix, to transform the encryption key. The transformed key cannot be directly used to decrypt the plain text. However, it can be used to recover the original encryption key.

The recovery of the encryption key from the transformed key takes a considerable amount of time. The author can choose the approximate amount of time it would take anyone to recover the original encryption key from the transformed key. The longer it takes to recover the encryption key, the more secure the diary is.

The author needs to choose two parameters: the amount of time she would like the diary to remain secure for and the amount of time she is willing to wait before she starts to recover the diary. These two parameters determine how long it will take the author to recover the diary. (The appendix describes the relationship between these three lengths of time.) For example, if the author wants to make her diary secure for 8 years and is willing to wait 30 years (from the time at which the diary was first encrypted) before she starts to recover the diary, the recovery process will take approximately 4 hours. In contrast, if she still wants to make her diary secure for 8 years but only wants to wait 10 years before she starts to recover the diary it will take her 9 months to recover the diary.

To find the encryption key under most encryption schemes, one can conduct an exhaustive search for all possible keys. Therefore, it would be helpful to use multiple computers to search for the correct key. The scheme described in this paper eliminates the benefit of using multiple computers to recover the encryption key.

Moore's Law states that computer speed doubles every eighteen months. This paper uses Moore's Law to estimate the length of time a diary is secure. However, computer speed might increase faster than Moore's Law estimates. To circumvent this problem, this paper proposes a scheme that allows the author to incrementally encrypt the diary at any future time. For example, suppose that one year after the President has started keeping and encrypting her diary, IBM perfects quantum computing which causes computer speeds to increase tenfold. The security of the President's diary will now be greatly reduced.

However, the President could overcome this problem by strengthening the diary's encryption so that it becomes as secure as it was before IBM's technological breakthrough.

4. Conclusion

This paper proposes a practical method by which a president or another government official can keep a diary and be reasonably confident that no one can read it while they are still in office. The longer the author is willing to wait before anyone can read the diary and the more time that can be devoted to decrypt the diary, the more secure the diary will be while she is in office.

Appendix

This appendix provides a detailed technical description of how to create a subpoena-proof diary.

Part A. Encrypting the Diary

This paper describes an encryption scheme for keeping a diary. It then describes how to apply this scheme for a subpoena-proof diary. Denote the diary by D and the length of the time to keep the diary secret by T.

Generate a composite number n= pq, where p and q are two large (e.g. 300-bit) randomly-chosen primes.

Compute m=(p-1)(q-1).

Choose t to be the number of the squaring module n operations that the computer can perform in time T.

Pick a random key K for a conventional cryptosystem, such as Data Encryption Standard (DES). This key should be long enough (e.g. 256 bits) so that searching for it is infeasible, even with the advances in computer speed expected within time T. Encrypt D with key K using DES encryption algorithm: D_k=DES(K, D)

Pick a random number a modulo n (with 1<a<n), and compute K'=K+ a^{2^t} (mod n). This step can be done efficiently by first computing e=2^t (mod m) and then compute b=a^e (mod n).
Save n, a, t, K', D_k. Discard the rest.

Part B. Decrypting the Diary

Two known approaches to decrypt the diary.

1. Find the DES key K by exhaustively searching from all possible keys of 256 bits.

Since K is 256 bit long, searching for it is infeasible even with the advances in computer speed expected within time T.

2. Find the DES key K by using K' and compute

b= a^{2^t} (mod n)

There are two known ways to compute b:

Compute m=(p-1)(q-1). Then compute e= 2^t (mod m).

Finally, compute b= a (mod n).

However, given n, finding m is probably as hard as factoring n. Mathematicians have been trying to factor large numbers for at least 3000 years and no efficient algorithm has been found. For example, factoring a 600-digit number requires 10^{55} years of computer time assuming the best known algorithm and a computer with 1-μsecond instruction time. Even if computers continue to get faster by an order of magnitude per decade and we can use most of the computers in the Internet, it will be centuries before factoring 600-bit number becomes feasible.

Compute b by starting with a and sequentially performing squaring modulo n operation t times.

Therefore, approach 2(b) is the only feasible way. Furthermore, by varying value t, we can control the time that the diary D can be decrypted. This is because repeated squaring seems to be an 'intrinsically sequential' process. No one knows a way to parallelize it since each squaring needs the result of the previous squaring. Having many computers is no better than having one. Although having a fast computer is better than having a slow one, the degree of variation in computation speed of a single computer can be estimated in accordance with the technology, while the computation speed of a parallel computer or many computers on the Internet combined depends on one's budget.

Part C. Choosing the Parameter To Ensure the Desired Security

To ensure that the diary is secure within 8 years and the diary can be recovered within 4 hours in 30 years, we need to choose t to satisfy the following conditions.

Condition 1. Within 8 years of the presidency, no computer can decrypt the diary even if the president gets subpoenaed.

Condition 2. It takes only 4 hours to decrypt the diary using an average-speed computer after 30 years.

To satisfy condition 1, one can assume a high-speed computer and the computer cannot decrypt the diary in 8 years time even if the computer is dedicated to decrypting the diary. Suppose S_i is the maximum number of squaring module n operations that a high-speed

computer can perform in the ith year during the next 8 years. Then t has to satisfy: $t > \sum_{i=1}^{i=8} s_i$, where one assumes that the computer is upgraded every year for this purpose. According to Moore's Law, the computer speed doubles every 18 months. To be conservative, we assume that the computer speed doubles every year, i.e., $S_{i+1}= 2S_i$. Therefore, $t>255\ S_1$.

To satisfy condition 2, one has to ensure that an average-speed computer (30 years later) can decrypt the diary within 4 hours. In other words, $t < S_{30}/6/365 = S_{30}/2190$. According to the Moore's Law, $S_{30} \approx 10^6\ S_1$. Therefore, $t < 456\ S_1$.

Therefore, we can choose t to be between $255\ S_1$ and $456\ S_1$. Note that we might want to be conservative in estimating the increase of the computational speed to ensure the timely recovery of the diary. In the next section, we present the scheme to increase the security of the diary when the computer speed is increased in at an unexpected rate.

Part D. Incremental Encryption

If the computational speed increases at an unexpected rate, the diary can be encrypted one or more times to ensure its security within 8 years. This can be done as follows: Choose a big t_1 that ensures the diary's secrecy within 8 years according to the current estimate and big enough key K_1. Perform the same mathematical operation on K_1 using a large composite number $n_1= p_1\ q_1$ and a_1 to get K'_1. Note that p_1 and q_1 are randomly-chosen large primes and a_1 is a random number modulo n_1. Use K_1 to encrypt D_k. Save the encryption result as $D_{k,,k1}$. Save $n, n_1, a, t, t_1, K', K'_1, D_{k,,k1}$.

To recover the diary, we first need to find K_1 and then decrypt $D_{k,,k1}$ to D_k. Finally, find K and then decrypt D_k to D. Note K and K_1 can be found in parallel. Therefore, the time it takes to recover the diary can be controlled by t_1.
Such an incremental process can go on as many times as needed, i.e. if computer speed increases suddenly.