Rechov Shaulson 59/6
Jerusalem 95400
Israel
September 11, 2009

Mrs. Patricia Byrne
P.O.B. C
East Corinth, Vermont
U.S.A.

Dear Mrs. Byrne,

My name is Moshe Rubin, a 52-year old software engineer living in Jerusalem, Israel. You may recall our phone conversation of August 9, 2009. Before proceeding, allow me to express my condolences to you on the passing of your husband, John. As a married person myself, I can imagine the magnitude of losing one's lifelong companion. May I wish you good health and a long life.

In our phone conversation, you requested I send you a letter explaining my reason for calling you.

Background

For the past 35 years I have been an avid amateur cryptologist. I first encountered John F. Byrne's "Chaocipher" in the early 70's in "Silent Years" and have been fascinated by the cipher ever since. Over the years I have looked at the Chaocipher challenge messages but put off attacking the cipher for a later date.

Exactly a year ago I decided to tackle the Chaocipher challenge messages in earnest. After analyzing the ciphers and making significant discoveries, I created a dedicated web site on the Internet and published my findings to the world. The goal was to stimulate more interest in solving the Chaocipher system. I am happy to say that several other amateur cryptanalysts have joined the effort. (Just 'Google' the word 'Chaocipher': the *Chaocipher Clearing House*, my web site, is the first match in the list.)

Last August the thought occurred to me that time is marching forward and none of us is getting younger. I decided to track down, and speak to, your husband John. My intention was to convince him to consider making the Chaocipher mechanism public in the hope of proving, once and for all, whether there was still commercial value in the system. My main point was to credit his father, John F. Byrne, in cryptologic history as the inventor of a novel cryptographic phenomenon, regardless of whether the Chaocipher could be marketed in the 21st century or not.

My overriding consideration was how to fully protect the rights to the Chaocipher concept within your family while, at the same time, putting Chaocipher to the ultimate test by opening it up for public scrutiny.

It is my personal opinion that the Chaocipher mechanism in its original form, although probably a secure cryptographic system for the first half of the 20th century, would not withstand the onslaught of modern cryptanalysis and computers today. I also believe that your father-in-law discovered a most original and interesting cryptologic concept which has stymied many researchers all these years. If his concept is truly novel he should go down in history as its discoverer.

Mrs. Byrne, I wish to impress upon you that I have no wish to cause you any financial loss or pain whatsoever. My only interest is in investigating the cryptologic concept called Chaocipher. I would never, in any shape or form, want to do so by ill-advising you or 'tricking' you in any way. As a G-d-fearing person I answer to a 'higher authority'.

Patenting Chaocipher

After our phone conversation I took the liberty of contacting Dr. Marc Berger, a wonderful G-d-fearing patent attorney living in Israel with whom I have worked closely over the past 15 years (please see the references page at the end of this letter for details about Dr. Berger). I asked Dr. Berger whether you could protect your intellectual property by patenting Chaocipher. Dr. Berger wrote me the following:

> "In answer to your questions:
>
> 1. Yes, Mrs. Byrne can patent the Chaocipher principle, provided: (i) the patent application is enabling (i.e., someone who reads the application will know how to manufacture the apparatus), and (ii) the invention has not yet been disclosed to the public. And you can also try to broaden the invention as much as possible.
>
> 2. You can (i) offer Mrs. Byrne to file a patent application and assign all rights to her, (ii) not to disclose the invention until after the patent application is filed, and (iii) to be available for consultation in commercializing the Chaocipher.
>
> If you assist me in preparing the patent application (as you've done in the past), by providing diagrams and explanations, then the total cost including filing fees will be around $1,000."

I would advise you to patent Chaocipher in any case, no matter how you proceed from here. With Chaocipher research going on today, someone may solve the system and discover the underlying mechanism. In such a case, I believe that person could actually file a patent before you do and reap whatever commercial benefits may exist. Filing a patent will protect your rights to the Chaocipher concept in all events.

Dr. Berger wisely proposes broadening the invention as much as possible. It is certainly conceivable that a computer version of Chaocipher could be made significantly more secure than the mechanical version John F. Byrne envisioned. A well-written patent would expand the scope of the invention, both protecting you better and opening up possible commercial horizons.

In 1990, Louis Kruh and Professor Cipher Deavours collaborated with your husband on an article published in 'Cryptologia', a journal dedicated to cryptology. I am disturbed by the fact that neither Kruh nor Deavours advised your husband how to determine whether Chaocipher could be marketed or not. In my opinion, the first step should have been to patent the Chaocipher concept, thereby protecting your intellectual property in all cases.

As Dr. Berger writes above, should you want help in preparing the patent application I would be more than happy to help. The patent would be assigned exclusively to you; I would not want any compensation. My interest in Chaocipher is purely historical and intellectual, and I would consider it an honor to help you, your late husband, and his father see Chaocipher finally move forward in the world.

I would be more than happy to assist if you would like the woman you've hired to contact me with any questions she may have. Should you consider filing a patent, you might want to consider the fact that Dr. Berger and I both live in Israel and can interact face-to-face. I am not a professional security consultant, but I believe my cryptologic background, and my access to excellent professionals like Dr. Berger, will enable me to assist you.

Testing Chaocipher's Marketability

Your father-in-law, John F. Byrne, was absolutely convinced that disclosure of the Chaocipher mechanism would not help a cryptanalyst in the least. For your reference I enclose two citations that stress this point:

1. A memorandum from John F. Byrne to G. M. Campbell of Bells Telephone, written in 1942, where Byrne writes in a handwritten footnote "*P.S. I wanted to emphasize the point that possession of my machines – with full knowledge of its principles and methods of operation – would not be of the slightest help in any attempt at decipherment.*"
2. In "Silent Years", chapter 21, page 266, paragraph 1: "… *yet possession of my device together with knowledge of the general principle involved, would not enable any person to decipher any messages whatever written by anyone else and not intended for him.*"

In our phone conversation you mentioned you had entrusted the Chaocipher information to a woman, the goal being to see if it could be marketed commercially. I am not a professional security expert, but I believe the following scenario is most likely to occur:

1. A considerable amount of money will be invested in the design and production of a Chaocipher device.
2. As soon as the device is marketed, thousands of talented and qualified cryptographers will attack the system, devising methods for breaking the cipher using modern-day computers. Given the physical device and the ability to encipher an unlimited number of messages, I cannot imagine that it could withstand the onslaught for more than a few days.
3. The device and mechanism will be declared insecure.
4. Whatever money was invested will be lost.

Once you are protected by a patent you can take the critical step of opening the Chaocipher mechanism to the cryptologic world. In this way the best cryptanalytic minds in the world would jump at the opportunity to prove or disprove its merits. There can be no false reports here. Within days or weeks you would know whether Chaocipher is indeed as secure as your father-in-law believed it was. Fully protected legally, you would know for certain whether it could be commercially marketed. If found to be commercially feasible you could then proceed to develop and market the product.

I would like to ask you if, once the Chaocipher patent is filed, you would allow me and my Chaocipher research colleagues to analyze the mechanism and publish our findings in a prestigious cryptography journal, most probably 'Cryptologia' (where your late husband published his joint article with Louis Kruh and Professor Cipher Deavours in 1990). Regardless of our academic findings, I believe your late father-in-law would receive the recognition due to him for having been the first to discover his original principle. And with the patent in hand, you are always able to market the product at any time.

John F. Byrne's Recognition in History

There are people that have gone down in history for discovering highly original cryptographic inventions. Two such people are Thomas Jefferson and Sir Charles Wheatstone. Thomas Jefferson invented the wheel cipher, a unique and original concept that was way ahead of its time in the 18th century, while the British Sir Charles Wheatstone invented the Playfair cipher and the Wheatstone cryptograph in the 19th century.

Truth be told, all three cipher systems just mentioned have been broken and would never be used for a commercial system today. Nonetheless both Jefferson and Wheatstone bask in the historical glory of having been the first to discover these important concepts.

It is my personal opinion that the Chaocipher mechanism, probably a secure cryptographic system for the first half of the 20th century, would be found to be insecure by modern cryptanalysts. I also believe that your father-in-law did discover a most original and interesting cryptologic concept which has stymied many researchers all these years. If his concept is truly novel he should go down in history as its discoverer.

Conclusion

I would like to apologize for my long letter, but there is much to say on these matters. The most important point in my letter is that you should seriously consider filing a patent for Chaocipher. If you wanted any assistance in doing so, wording it in the best possible way, I would be more than glad to be of help.

With best regards,

Moshe Rubin

P.S. I can always be contacted by any of the following means:

Moshe Rubin
Rechov Shaulson 59/6
Jerusalem 95400
Israel

Home: +972-2-6520160
Cell: +972-54-4832999

mosher@mountainvistasoft.com
moshe.rubin@gmail.com

References

I realize that you don't know who I am, although I have been intimately aware of John F. Byrne and your husband John Byrne for more than 30 years. Below please find material you, or anyone else, can look up on the Internet to enable you to find out more about myself and Dr. Marc Berger.

Moshe Rubin

The following text was retrieved (September 9, 2009) from the web page http://www.mountainvistasoft.com/author.htm :

> Moshe Rubin, the author of Fathom It!, is a Research Scientist at Yonatan Labs in Ra'anana, Israel. He holds a B.Sc. in Computer Science, and has been a Windows programmer since the days of Windows 2.0 (a long time ago!).
>
> When not occupied with his professional work or improving Fathom It!, he has been known to publish technical articles in prestigious magazines, such as Windows Tech Journal and Windows Developer's Journal. He is the former contributing editor of the "Battleships" puzzle column in the "GAMES" and "World of Puzzles" magazines, and provides Solitaire Battleship puzzles to puzzle publishers around the world.
>
> His other interests are playing the English Concertina and Classical Guitar, researching and blogging about classical cryptanalysis, and trying to explain the intricacies of Fathom It! to his wife Rochelle and children (Nachum, Chani, Dvora, Tzivya, Shoshana, Elisheva, Betzalel, and Malka Bracha).

A photograph of myself and accompanying text (related to my lifetime love of the English Concertina) can be found at http://www.mountainvistasoft.com/concert.htm .

Dr. Marc Berger

The following text was retrieved (September 11, 2009) from the web page http://www.iseemedia.com/about/management.html :

> **Marc A. Berger**
> **Chief Scientist**
>
> Marc Berger serves as patent agent for several companies in the software industry. Berger was formerly Chief Scientist of MGI Software, Corp., where his responsibilities included intellectual property, technology evaluation, and liaison with industry consortia and standards bodies. Prior to MGI, Berger was Chief Scientist for Live Picture, Inc. and for OliVR Corporation, Ltd., an Israeli software firm that specialized in digital image compression and processing tools. Berger is also a consultant for the Weizmann Institute of Science, and served as Chairman of the Technical Committee and board member for the International Industry Imaging Association (I3A – formerly the Digital Imaging Group). Earlier Berger was on the faculty at Carnegie Mellon University and Georgia Institute of Technology. He was an appointed member of the US National Research Council (NRC) Panel for the Assessment of the National Institute of Standards and Technology (NIST).