value was not there for most users, versus anticipated issues with hardware drivers, and software that would need to be replaced, purchased, or added. This OS became viewed as unsuitable, for those and the other reasons. Sales of new computers would take a nosedive and never recover.

Lefty was concerned if MS could correct itself with the next version of windows, but was optimistic in spite of everything, that they could and would.

Windows 8 also disappointed some in that little had been done to advance the state of the art regarding privacy and encryption.[109] The Internet continued to evolve to become more dangerous for both computers and users. Some wanted Microsoft to develop and implement an easy system to use PGP encryption for email security.

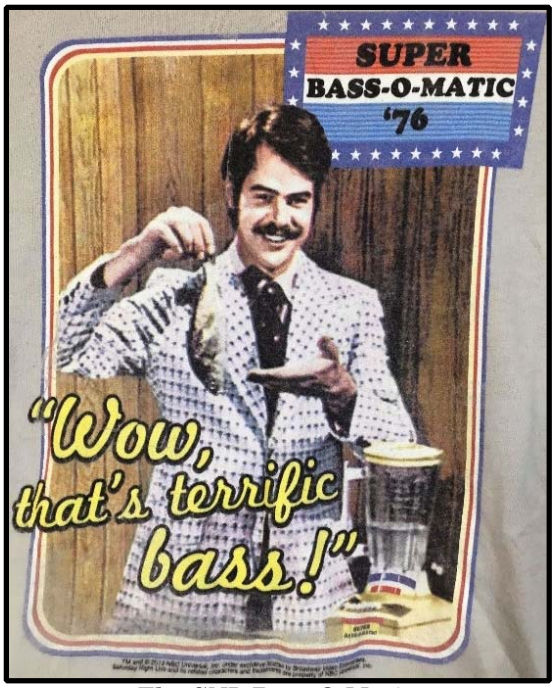
Cryptology pioneer Phil Zimmermann

Phil Zimmermann was the creator of Pretty Good Privacy or PGP, the most widely used email encryption software. Lefty had first met Phil while at IBM and was also attending school in the evenings. Phil was earning a B.S. degree in computer science there in Boca Raton. He later moved to the San Francisco Bay Area, and they kept in touch during Lefty's brief internship at Intel in nearby Santa Clara. Phil once told him that the definition of a Nerd was "someone who had found something more interesting than sex."

---

[109] *In cryptography, encryption is the process of encoding a message or text in such a way that only authorized parties can access it. The intended information or message, is encrypted using an encryption algorithm, generating ciphertext that can only be read or accessed if first decrypted.*

Phil wrote the popular Pretty Good Privacy or PGP program, then made it available including the source code, through public FTP[110] for downloading. This was the first widely available program to implement public-key cryptography. Shortly thereafter, the software spread uncontrollably via the Internet. The first PGP version included an encryption algorithm developed by Zimmermann; which he called Bass-O-Matic[111].



The SNL Bass-O-Matic

After a report from RSA Data Security, Inc., in a licensing dispute regarding use of the RSA algorithm[112] in PGP, the United States Customs Service initiated a criminal investigation

---

110 *The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.*
111 *The name is explained in his comment in the source code: "BassOmatic gets its name from an old Saturday Night Live skit involving a blender and a whole fish. This algorithm does to data what the original Bass-O-Matic did to the fish."*
112 *An algorithm is a piece of computer code with a self-contained sequence of actions to be performed. Software algorithms perform calculations, data processing and automated reasoning tasks.*

of Zimmermann, for allegedly violating the Arms Export Control Act. The United States Government regarded cryptographic software as a munition, and thus was subject to arms trafficking export controls. At that time, the boundary between cryptography permitted "low-strength" and cryptography impermissible "high-strength" for export from the United States; put PGP on the too-strong-to-export side of the boundary. The investigation lasted three years, pretty much destroyed Phil financially and emotionally for a time, but then the case dropped without the filing of any charges. The boundary for legal export of software was later raised, to allow PGP export.

The government dropped its case without indictment in early 1996, and Zimmermann founded PGP Inc. to release an updated PGP version. After acquisition by Network Associates (NAI), Zimmermann stayed on as a Senior Fellow. NAI later decided to drop the product line, and PGP reacquired from NAI by a company called the PGP Corporation. Zimmermann then served as a special advisor and consultant. Symantec later acquired the PGP Corporation. Zimmermann is a fellow at the Stanford Law School's Center for Internet and Society. He is a principal designer of the cryptographic key agreement protocol (the "association model") for the Wireless USB standard.

A 2013 article titled Zimmermann's Law, quoted Zimmermann saying, "The natural flow of technology tends to move in the direction of making surveillance easier, and the ability of computers to track us doubles every eighteen months". His words became prophetic later that year in the wake of documents released by Edward Snowden, published by Glen Greenwald and others regarding the NSA's massive surveillance of the American people and others worldwide.