

Data Insecurities: Why Equifax Hasn't Been Credit Worthy. "Holds Information on 800 Million Consumers and almost 90 Million Businesses"

By [Greg Guma](#)

Global Research, September 14, 2017

Region: [USA](#)

Theme: [Intelligence](#), [Law and Justice](#),
[Police State & Civil Rights](#)

It should not come as a shock that Equifax, one of the three big agencies that track credit status, has failed to protect the data it has on 143 million people. Nor should it be surprising that the company didn't inform its affected customers for six weeks after discovering that hackers had gained access to their private information. Collecting, selling and sometimes misusing mountains of sensitive data for decades, Equifax has evidently become too big to care.

Instead, three executives sold \$1.8 million of their company shares days after the company discovered the problem, more than a month before it was made public.

"If that happened, somebody needs to go to jail," threatened **Sen. Heidi Heitkamp**, a Democrat on the Senate Banking Committee.

In the days following the breach announcement Equifax shares dropped 20 percent.

At first, the company wanted customers to pay for a freeze to their accounts. That would protect their personal data. But after a deluge of complaints, the offer changed, with Equifax opting instead to waive fees for customers who want to freeze their credit files — but only until November 21. Going forward, it could face the largest class action lawsuit in history, with the potential to bankrupt the company.

When I first looked into Equifax in 1978, it was already a corporate force, with 1,800 offices, 14,000 employees, and a nationwide investigative system maintaining dossiers on 46 million people. The oldest of the three largest US credit agencies, it had revenues of \$275 million a year. Equifax's services at the time ranged from credit reporting, insurance investigations and underwriting to motor vehicle data tracking and assorted "management system services" – aka private investigations.

Today Equifax holds information on more than 800 million consumers and almost 90 million businesses. Operating in 14 countries it produces annual revenues of more than \$3 billion. On the other hand, the employee roster is down to about 9,000.

Founded in 1899, Equifax had not fully committed to computers by the late 1970s. But an industry transition was underway. In Vermont, the Credit Bureau of Burlington had taken an early lead, working with Trans-Union Systems, a national computer network used by retailers and credit card companies. Data flowed in multiple directions, with stores seeking

information on potential customers and other clients using the data those businesses amassed.



1978 investigative feature

Before the digital age, collecting information and creating a customer profile — to establish what was known as “creditworthiness” — involved a larger staff and considerable legwork. For Equifax “field investigators” it meant conducting interviews, with the subject as well as friends and neighbors. From courts and police departments they gathered any criminal information, while desk-bound staffers clipped newspapers and gathered reports. To complete a dossier, an investigator might talk to your employers, hunt down old government records, or even strike up conversations with local shop keepers.

But mass producing customer dossiers (investigators worked on up to 40 a day), particularly profiles that included not just hard data but also tidbits of gossip, could lead to mistakes and abuses. Creditworthiness was a slippery concept, an imprecise composite of job patterns, credit and bank accounts, character, habits, family status and morals. As a result, Equifax was hit with a batch of lawsuits during the 1970s, losing some and quietly settling others.

One Michigan woman collected \$321,000 when the company falsely reported that she was an excessive drinker. Another woman from South Dakota won a settlement when Equifax said that the money for her new Chevy had come from prostitution — also proven false.

There was also the California insurance broker who won \$250,000 when Equifax investigators alleged she was dishonest. In New Jersey there was trouble when State Farm refused coverage to a Princeton faculty member after Equifax reported (accurately but irrelevantly) that she was living with a man “without the benefit of wedlock.”

At times, Equifax operated like a private detective agency. In at least one case, it was caught helping a corporation to obtain gossip about a critic. An executive at American Home Products, a major drug manufacturer, had hired the company to dig into the personal affairs of Jay Constantine, a congressional staffer who was helping to write legislation opposed by Big Pharma.

This was before the Retail Credit Company of Atlanta, Georgia changed its name to Equifax. After 77 years in business, the 1976 rebranding was prompted by all the bad press, including a Federal Trade Commission lawsuit filed in 1975. The charges, as outlined for me by an FTC staffer, included illicit use of consumer information, failure to disclose terms, and false and misleading advertising.

The technology of data gathering has changed since then, but the shabby tactics have survived. In 2000, Equifax, along with Experian and TransUnion, was fined \$2.5 million for blocking and delaying phone calls from consumers trying to obtain information about their credit. In 2013, a federal jury in Oregon awarded \$18.6 million to Julie Miller against Equifax for violations of the Fair Credit Reporting Act.

In contrast, Equifax has had no problem sharing files and data with the FBI and other government agencies, according to **George O'Toole**, a former CIA agent. While reporting on Vermont's private intelligence industry, I was told that Equifax tended to hire ex-State Police officers, possibly because they might have access to government information that was off limits to the public.

Another ex-CIA operative, **Harry Murphy**, claimed that Equifax was especially useful to federal agencies. The draw was its enormous files of auto and life insurance applicants. Even back in the 1970s, however, big data transfers between public and private entities were difficult to control, and law enforcement and intelligence officers often moved into the private sector after retirement, or for the paycheck.

The emerging private dossier industry was run largely by law enforcement and intelligence alumni, an Old Boy Network that closely linked it with government operations. The data moved freely, but the potential for mischief was not widely recognized.

During my research into the activities of Equifax and other big data agencies, I also heard about an odd encounter with Earl Hanson, a Barre resident who applied for insurance with Colonial Penn Mutual. In return he received a letter from Equifax asking for more information about an auto accident he had forgotten to report. Hanson was cooperative, explaining all about hitting a deer. But the exchange made him curious to know what else they had discovered about him, from the Motor Vehicles Department or anywhere else.

After writing to the company's Dataflo center and to the New Hampshire branch office, however, Hanson was told that Equifax actually had no file on him. Unsatisfied with that response, he filed a complaint with the Attorney General's office. But the State lost interest, eventually closing the case, and Equifax didn't share any further information. As usual, it was too big to care.

Greg Guma is the Vermont-based author of *"Dons of Time," "Uneasy Empire," "Spirits of Desire," "Big Lies,"* and *"The People's Republic: Vermont and the Sanders Revolution."* His latest book is *"Green Mountain Politics: Restless Spirits, Popular Movements."*

This article was originally published by [Greg Guma / For Preservation & Change](#).

The original source of this article is Global Research
Copyright © [Greg Guma](#), Global Research, 2017

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Greg Guma](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca