



# Equifax and the Latest Round of Identity Theft Roulette

Hal Berghel, University of Nevada, Las Vegas

*The Equifax data breach has exposed nearly half of the US adult population to identity theft, but that's not the real story.*

**T**he recent Equifax data breach that revealed personal data on 145 million people—nearly half of the US adult population—has been a staple of the commercial media diet for several months. However, the important story lies deep below the crude facts reported in the headlines and requires considerable digging.

This security breach supposedly resulted from a known vulnerability in the Apache Struts server software that had been announced in early March 2017 by many of the major security-breach reporting sites. Technically speaking, the Struts parser had incorrect exception handling during file uploads that created an attack vector through execute commands via the #cmd in content-type HTTP headers (nvd.nist.gov/vuln

[/detail/CVE-2017-5638#VulnChangeHistoryDiv](#)). According to former Equifax CEO Richard Smith's 3 October 2017 congressional testimony, the company was notified of the available patch on 8 March, and the following day an internal email was sent out—from whom he didn't say—instructing the IT staff to apply the patch within 48 hours (docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf).

Equifax apparently didn't apply the patch until its online dispute portal had been compromised three months later. Subsequently, Smith, along with the company's CIO and CISO, were sent into forced retirement.<sup>1</sup> In an all-too-familiar corporate scenario, Smith received a \$90 million golden handshake that, according to *Fortune* magazine, averages "63 cents for every customer whose data was potentially exposed."<sup>2</sup> Three other Equifax executives sold \$1.8 million in Equifax stock (about 10 percent of their holdings) just prior to the company's public notification of the hack, so far without repercussion.<sup>3</sup> I'm confident that these aren't the kind of capitalistic practices that Adam Smith endorsed so confidently.

This much has been widely reported. But the story just starts there.



## IDENTITY THEFT ROULETTE

Equifax has managed to distinguish itself notoriously in many ways, starting with the sloppy oversight of the IT department that delayed patching the software in the first place. How many information security policies have you seen that recommend applying patches and hot fixes whenever you get around to it? Added to this was a five-week delay in reporting the data loss to the public—at this point, approximately six months after the announcement of the vulnerability and availability of the patch. Then Equifax outdid itself by creating an insecure, third-party complaint registration website that bungled the TLS certificate revocation check.<sup>4</sup> But the icing on the cake was Equifax's requirement that in order to sign up for their free one-year credit monitoring service—necessitated by a data breach resulting from their own incompetence—you had to agree to a forced arbitration clause, forfeiting your rights to sue the company for any harm you might suffer. After the public, the attorney general of the State of New York, and Senator Sherrod Brown (D-OH) cried foul, Equifax rolled back the litigation waiver but only if you contacted them in writing within 30 days.<sup>5</sup> Sherrod spoke for everyone in observing, "It's shameful that Equifax would take advantage of victims by forcing people to sign over their rights in order to get credit monitoring services they wouldn't even need if Equifax hadn't put them at risk in the first place."

Given the irresponsible management that has overtaken the financial industry in the past 50 years (do the S&L crisis and Great Recession of 2008 ring a bell?), perhaps Equifax's behavior shouldn't be surprising. The incident is also a stark reminder of how feckless federal regulations are in establishing sound corporate IT security practices. There's little evidence of modern best practices in Equifax's

handling of this breach—from ignored patches to outsourcing the customer inquiry website to outsourcing the remediation website to a third party that bungled TLS certificates.

But let's peek further behind the corporate veil. According to *TechCrunch*, former CEO Smith blamed the patch failure on some unnamed individual in IT.<sup>6</sup> He told Congress that "the breach occurred because of both human error and technology failures," but failed to mention the most likely culprit: poor corporate leadership, inconsistent managerial oversight, and a corporate culture that underemphasized the importance of computing security and risk

management officer in this case? How did the initial demand for, and quick removal of, an arbitration clause for credit monitoring in one week pass muster with the general counsel? What masqueraded for an information security policy at Equifax? Where were the internal security checks?

Even with the soundest security practices, not every data breach can be prevented. But there's no excuse for a breach involving so much sensitive personal data caused by failing to fix a known vulnerability with a ready-to-use patch. We've seen this kind of thing before—recall the 2012 South Carolina Department of Revenue hack,

The Equifax breach reveals just how much companies are willing to irresponsibly gamble with our personal information.

management. Whether this underemphasis was the result of unqualified personnel, inadequate security, IT budget cutbacks, or some other area of C-level irresponsibility has yet to be reported.

But one thing is evident: a company with clear, established security policies built on industry best practices that has a trained and experienced security staff normally doesn't experience a breach of this magnitude, and it most definitely doesn't react this clumsily. Industry standard information security practices dealing with data classification and retention, encryption, segregation of data assets, patching and update policy, incident response policy, and so forth have been codified for several decades (for example, BSO7799-ISO17799, ISO27000 and ISO/IEC 27001, COBIT, FISCAM, PCI DSS). The SANS Institute has been offering classes in these areas for nearly 30 years. Where was the risk

where incompetence reigned supreme at every level of state government<sup>7</sup>—but never on this scale. The Equifax breach reveals just how much companies are willing to irresponsibly gamble with our personal information.

## RAMIFICATIONS AND PROGNOSTICATIONS

About five weeks after disclosing the data breach, Equifax lost a \$7.25 million IRS sole-source contract to provide antifraud prevention (the irony of this award shouldn't be overlooked).<sup>8</sup> On the positive side, the Government Accountability Office (GAO) put the kibosh on the contract with a company that didn't deserve it and probably couldn't implement it securely. On the negative side, the government's sloppy due diligence was revealed in the report of cancellation. The contract was originally offered to Experian for 10 percent of Equifax's bid, but Equifax

appealed the decision, and the IRS initially caved to the pressure. By mid-October 2017, following a storm of public and congressional protest, the GAO had finally had enough bad press over the Equifax contract and pulled the plug. But the GAO only took this action after it no longer feared reprisal from Equifax lawyers and lobbyists, not when Equifax contested the Experian award for a 900 percent cost increase. And as we now know, the IRS awarded the sole-source contract in the first place with dubious justification.

The current wave of bipartisan political opportunism to discredit Equifax is bothersome—not that the company doesn't deserve it, mind you, but that the ruling elite withheld their criticism until the data breach provided them with political cover. (Likewise, no one said anything about Bernie Madoff's Ponzi scheme until it became politically fashionable to bash him.)

Equifax's stock lost 30 percent of its value in the month following announcement of the breach<sup>9</sup> but has since partly rebounded ([secure.marketwatch.com/investing/stock/EFX](https://secure.marketwatch.com/investing/stock/EFX)). The company also faces hundreds of millions of dollars in fines, lawsuits, and regulatory costs, though one Wall Street analyst predicted that “we do not expect such expenses would be material to [Equifax's] financials.”<sup>10</sup> But even if the company weathers the storm and is spared the well-deserved corporate death penalty,<sup>11</sup> it has lost all of its credibility. The ultimate cost to the citizen-victims might never be determined. The impact of the release of so much personally identifiable information (PII) on retirement programs, the victims' credit, future voter registrations and the like is incalculable. Because of these potential consequences alone, it's worthwhile identifying the real problem—and that has nothing to do, strictly speaking, with this data breach.

## THE NEW LOCHNER ERA

The first 40 years of the 20th century are commonly called the Lochner Era by legal historians. *Lochner v. New*

*York* was a 1905 Supreme Court case in which the five conservative justices in the majority applied the principle of substantive due process—extending the Fourteenth Amendment's due process clause to include the right to freedom of contract—to prevent the State of New York from regulating working hours for bakers. For the next four decades, freedom of contract was a staple in SCOTUS decisions and the poster child for legislating by judiciary.

An analogous situation exists today in what I'll call the Too Big to Fail Era. A major deflection point in this era began in 1999 under President Clinton with a memo by then US Deputy Attorney General Eric Holder that discouraged federal prosecution of financial crimes when the accused institution is so large that its failure might damage the economy. Under the rubric of giving the judiciary greater prosecutorial and sentencing flexibility, Holder's memo sent Wall Street the signal that larger corporations would enjoy special dispensation from the Justice Department if only their misdeeds are large enough. The memo joined another Clinton-era policy shift, repeal of the Glass-Steagall Act, which ended the congressionally mandated separation of commercial and investment banking since 1933 and set the stage for the reckless corporate behavior that led to the 2008 recession.<sup>12,13</sup> More far-reaching was the enormous moral hazard that these two actions placed on the public and the economy.

The Equifax incident under review is just the latest manifestation of this moral hazard. The real problem is that the US has failed to deal effectively with the ownership of personal information. There's no right to privacy in our Constitution, and what little protection that may be derived is subsumed under the shadowy “penumbra” alleged in 1965 by Supreme Court Justice William O. Douglas in his opinion in *Griswold v. Connecticut*. Although some constitutional right to privacy seemed evident to the other justices in the majority, there was no

consensus on where the epicenter might be found in the Bill of Rights. Justices Byron White and John Marshall Harlan II thought they saw it in the Fourteenth Amendment's due process clause; Justices Arthur Goldberg, William Brennan, and Chief Justice Earl Warren spotted it in the Ninth Amendment; and Justice Douglas perceived emanations from the freedom of speech and association provisions of the First Amendment and the self-incrimination clause of the Fifth.<sup>14</sup>

Most neoliberals and conservatives have never accepted a right to privacy in any interpretation of the Constitution—literal, original, or otherwise. And so it is with the right to own personal information about ourselves. Equifax and the other credit reporting companies have taken advantage of this lack of right to ownership, and simply purloined PII for their own business purposes without risk. The procorporatists in politics are unyielding in their support of the rights of business over those of citizens. When you think about it, that's always been the case in the US, but the digital age has made the situation much worse.

If harmful data breaches are to be stopped, we need to resurrect Glass-Steagall and once again hold corporations—regardless of how big they are—responsible for the collateral damage that their activities produce. This could come in the form of a constitutional amendment that guarantees citizens a right to privacy (unlikely), legislation that holds corporations financially responsible for direct and consequential damages to victims of their data breaches (also not likely—the business lobbies and neoliberal politicians won't stand for it), or legislation that requires an expressed opt-in option by citizens for credit agencies, financial organizations, credit reporting companies, integrated marketing companies, information aggregators, nongovernmental agencies, and so on to retain PII about them in their databases.

An opt-in requirement might have a

## <ALT>-FAQs

In last month's Out of Band column, I wrote in defense of science and scientific research.<sup>1</sup> I pointed out that nonscience or antiscience has become weaponized in the last 50 years to support all manner of absurd ideologies, partisan policies, religious extremism, commercial interests, and so on. Occasionally, scientists inadvertently provide ammunition to the antiscience zealots. Such an occasion arose in the 15 May 2015 issue of *Physical Review Letters*.<sup>2</sup> In that issue, the good folks at CERN published a 33-page article on their work with the Large Hadron Collider. Based on this work, the authors published their estimate of the mass of the Higgs boson—a monumental achievement in physics to be sure, and one worthy of considerable recognition, but not in the form that they sought.

The problem is that the article has 5,154 coauthors.<sup>3</sup> The first 9 pages describe the research, and the next 15 pages list the authors. Such hyperauthorship in science and engineering isn't that unusual.<sup>4</sup> Everyone familiar with large projects realize that the number of critical contributors can easily run into the thousands. For example, a recent genomics paper has more than 1,000 authors, and a 2015 *Nature* article on rare particle decays has 2,700 coauthors. The problem is that listing too many coauthors—by my count, the CERN article has 573 authors per page or around one author per word—opens a project, and indeed the scientific community at large, to ridicule from antagonists. Using the CERN article as an example, one can imagine headlines like these emanating from the faux news outlets:

- » "How Many Scientists Does It Take to Write One Page of an Article? Answer: 573"
- » "Big Science Draws from the Government Pork Barrel Again—Each Scientist Contributed 1 Word in Recent Article"
- » "Academics Will Do Anything for Tenure: Recent 9-Page Physics Article Cites 5,000 Authors"
- » "Featherbedding in Science—5,000 Authors Listed on 9-Page Report"

Antiscientists are on the continuous prowl for nits to pick in furtherance of their agenda. I illustrated that point in my October 2017 Out of Band column when I discussed the distorted criticisms of the Truthy project.<sup>5</sup> Hyperauthorship provides just the right vehicle for detractors. While one might legitimately complain that the authors and publisher have blurred the distinction between the role of author and investigator, that's not likely to be the complaint from the dark forces attacking science. A far better way of achieving the recognition would be to use a pseudonym for the authors, simply cite the name of the project(s), provide a link to an author list, or put the list on the journal website as critical contributors. By the way, the pseudonym approach effectively served a group of mathematicians who collectively published under the name of Nicolas Bourbaki from the 1930s to this day ([www.britannica.com/topic/Nicolas-Bourbaki](http://www.britannica.com/topic/Nicolas-Bourbaki))—many of whose works remain classic texts in set theory and mathematics.

### References

1. H. Berghel, "The New Science Wars," *Computer*, vol. 50, no. 11, 2017, pp. 72–76.
2. G. Aad et al., "Combined Measurement of the Higgs Boson Mass in  $pp$  Collisions at  $\sqrt{s} = 7$  and 8 TeV with the ATLAS and CMS Experiments," *Physical Rev. Letters*, vol. 114, no. 19, 2015, pp. 191803-1–191803-33; [physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.114.191803](http://physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.114.191803).
3. D. Castelvecchi, "Physics Paper Sets Record with More Than 5,000 Authors," *Nature*, 15 May 2015; [www.nature.com/news/physics-paper-sets-record-with-more-than-5-000-authors-1.17567](http://www.nature.com/news/physics-paper-sets-record-with-more-than-5-000-authors-1.17567).
4. C. King, "Multiauthor Papers: Onward and Upward," *Science-Watch Newsletter*, July 2012; [archive.sciencewatch.com/newsletter/2012/201207/multiauthor\\_papers](http://archive.sciencewatch.com/newsletter/2012/201207/multiauthor_papers).
5. H. Berghel, "Net Neutrality Reloaded," *Computer*, vol. 50, no.11, 2017, pp. 68–72.

chance if Congress can catch the pro-business lobbyists off guard and the discussion is timed to avoid the most pressing campaign finance demands. The trick would be to write the legislation in such a way that takes advantage of an information taxonomy so that opt-in would mean different things in different contexts (Social Security numbers could only be used by the federal government and those

organizations required to report financial information, mother's maiden name could never be required at any time, Medicare numbers could only be required by healthcare organizations, and so on). But in any of its possible incarnations, opt-in as I use the term would amount to credit services by subscription: if you don't feel the need for a credit report, don't opt-in. That would force lenders and creditors to

actually practice what they preach: KYC (know your customers). In my own case, 100 percent of the accesses to my credit report in recent years were from companies who offered unsolicited credit. There's no possible interpretation of the Constitution that guarantees unsolicited credit issuers a right to access our credit reports!

In short, until such time that we can turn care, custody, and control of

personal information over to the individuals to whom it relates, we'll never be able to manage these data breaches. If we can't muster the political might to do this, the next best alternative might be to create some sort of government-operated information commons for PII where access would be given to selected fields only with customer permission.<sup>15</sup> If the federal government aggregated all of its PII from such agencies as the Social Security Administration, the Department of Homeland Security, and the IRS, as well as state and local governments, it would already have such an information commons. I'm not recommending this aggregation, but pointing out that much of the data already exists in government databases and if it's a choice between trusting Equifax, Credit Card Solutions, Heartland Payment Systems, or one of the other companies involved in massive data breaches on one hand, or some bureaucratic government agency on the other, I'll take the bureaucratic government agency any day.

To illustrate my point, read the last two pages of Richard Smith's previously cited congressional testimony, where he envisions a "new" paradigm for secure credit reporting services. His idea of pace-setting innovation is to actually allow consumers to control access to their credit records. Now that's inspired thinking! But he neglects to mention that customers had such control before companies like his began their Orwellian data collection and abusing Social Security numbers as candidate keys in their databases. Next, he suggests beginning a dialogue on replacing SSNs as the "touchstone" for identity verification. Well, that dialogue has been taking place for over 50 years, but Smith apparently wasn't listening.<sup>16</sup>

**T**he solution to massive data breaches isn't to heed the recommendations of corporate executives who remain clueless as to the attendant risks of their business processes to the public, but to end the

game of identity theft roulette and look instead to the technical community for answers. **□**

REFERENCES

1. J. Surane, "Equifax Says CIO, Chief Security Officer to Exit after Hack," Bloomberg, 15 Sept. 2017; www.bloomberg.com/news/articles/2017-09-15/equifax-says-cio-chief-security-officer-to-leave-after-breach.
2. J. Wiczner, "Equifax CEO Richard Smith Who Oversaw Breach to Collect \$90 Million," Fortune, 26 Sept. 2017; fortune.com/2017/09/26/equifax-ceo-richard-smith-net-worth.
3. A. Melin, "Three Equifax Managers Sold Stock before Cyber Hack Revealed," Bloomberg, 8 Sept. 2017; www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack.
4. D. Goodin, "Why the Equifax Breach Is Very Possibly the Worst Leak of Personal Info Ever," Ars Technica, 7 Sept. 2017; arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever.
5. D. Dayen, "Equifax Is Proving Why Forced Arbitration Clauses Ought to Be Banned, Just Like the CFPB Wants to Do," The Intercept, 8 Sept. 2017; theintercept.com/2017/09/08/equifax-is-proving-why-forced-arbitration-clauses-ought-to-be-banned-just-like-the-cfpb-wants-to-do.
6. S. Buhr, "Former Equifax CEO Says Breach Boiled down to One Person Not Doing Their Job," TechCrunch, 3 Oct. 2017; techcrunch.com/2017/10/03/former-equifax-ceo-says-breach-boiled-down-to-one-person-not-doing-their-job.
7. H. Berghel, "The SCDOR Hack: Great Security Theater in Five Stages," Computer, vol. 46, no. 3, 2013, pp. 91-93.
8. D. Kravets, "Federal Watchdog Tells Equifax—No \$7.25 Million IRS Contract for You," Ars Technica, 16 Oct. 2017; arstechnica.com/tech-policy/2017/10/federal-watchdog-tells-equifax-no-7-25-million-irs-contract-for-you.
9. V. Reklaitis, "Equifax's Stock Has Fallen 31% since Breach Disclosure, Erasing \$5 Billion in Market Cap," MarketWatch, 14 Sept. 2017; www.marketwatch.com/story/equifax-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14.
10. E. Court, "Equifax Earnings: Breach May Have Hurt Consumers, but It Won't Hurt the Business," MarketWatch, 24 Oct. 2017; www.marketwatch.com/story/equifax-earnings-breach-may-have-hurt-consumers-but-it-wont-hurt-the-business-2017-10-23.
11. R. Fein, "Equifax Deserves the Corporate Death Penalty," Wired, 20 Oct. 2017; www.wired.com/story/equifax-deserves-the-corporate-death-penalty.
12. N. Prins, *It Takes a Pillage: An Epic Tale of Power, Deceit, and Untold Trillions*, reprint ed., SWN Books, 2013.
13. D.A. Stockman, *The Great Deformation: The Corruption of Capitalism in America*, PublicAffairs, 2013.
14. E. Lazarus, *Closed Chambers: The Rise, Fall, and Future of the Modern Supreme Court*, Penguin Books, 1999.
15. N. Kranich, *The Information Commons: A Public Policy Report*, The Free Expression Policy Project, Brennan Center for Justice at New York Univ. Law School, 2004; www.fepproject.org/policyreports/InformationCommons.pdf.
16. H. Berghel, "Identity Theft, Social Security Numbers, and the Web," *Comm. ACM*, vol. 43, no. 2, 2000, pp. 17-21.

**HAL BERGHEL** is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.