The Outsourcing of Payroll Data by the University of California and Why We Should Worry

Akos Rona-Tas
Professor of Sociology, UC San Diego

Summary:

UC outsources our payroll data to Equifax Workforce Solutions. Doing this, UC broke its 2007 promises and gave our data over to a company known for weak data security, poor customer service and its plans to aggregate our data with other information to use it in the interest of corporate third parties (employers, lenders, retailers etc.). UC should return to us the control of our data. It should cancel its contract with Equifax and let UCPath handle employment verifications.

Between 2013 and 2015, the University of California, has signed a series of contracts with the consumer credit agency Equifax, outsourcing our employment verification to Equifax Workforce Solutions (TALX until 2012), a subsidiary of Equifax. UC employees in the past could receive an employment verification letter from their campus, most recently through their At-Your-Service Online (AYSO) site. Currently, this option is still available, however, by the contract, employment verification (often requested for bank loans or by prospective employers) will soon be handled at all campuses through Equifax's web site: The Work Number (TWN).

Currently, all but two University of California campuses participate in the outsourcing. UC Santa Cruz and UC Berkeley are supposed to join the other campuses in the near future.

There are at least three reasons that this is cause for serious concern. The first has to do simply with *data security*. Recent security breaches at Equifax compromised 147 million records. Earlier, smaller breaches resulted in the theft of tens of thousands of employment files. The second is the *customer service* record of Equifax. Equifax has the worst record of consumer complaints with the Consumer Finance Protection Bureau (CFPB). And the third, *data aggregation*, is probably the most worrisome. Equifax purchased TALX in order to aggregate employment data with data from other of its subsidiaries, including its credit registry. Weak security, poor service and big data aggregation are the three chief concerns that I will address below.

All three are rooted in one simple cause: **people like you and me (the faculty and staff of the university) are not the customers of Equifax. We are just its data, its product. Equifax's business depends not on the people whose data it sells but on employers and lenders who provide and use their data.** [1] The UC-Equifax contract takes away most of our ***control*** over our own data.

[1] One of the services of TALX/Equifax Workforce Solutions is to represent employers fighting unemployment claims by ex-employees.

While those three problems burden faculty and staff individually, there is also the question whether this contract makes any sense as an economic proposition for the university as a whole. UC pays Equifax for accepting our data and TWN site then charges for each inquiry (except when one looks at one's own record). I will not be able to address this question, and this is a secondary issue, in any case. But UC is about to complete the UCPath Project, [2] that will centralize all HR functions at UC and it is unclear why Equifax needs to be inserted between verifiers and UCPath.[3]

Background

More than eleven years ago, on December 18, 2006, UC employees of all campuses except Berkeley, UCSC and UC Irvine, received an email message about new tax services offered through TALX, a private payroll service company that at that time was independent. We were told that our payroll data will be sent to TALX and we can download our W-2 form from TALX. If we wanted to opt out of this service individually, we were given until January 1, 2007 to do so.

The faculty at several UC campuses revolted not just against the idea of handing our data to a private company but also against the process that not just failed to consult faculty (or other employees) but was clearly designed to minimize our ability of opting out. Our fears deepened, when on February 14, 2007, TALX announced it was going to be bought by Equifax, one of the three giant credit bureaus, for $1.4 billion. Next day, in an earnings call, Richard Smith, CEO of Equifax, explained to investors that TALX data will be used to improve Equifax credit files.

Local academic senates protested the deal and brought the issue to the systemwide Academic Council that discussed it and expressed its own concern to the Office of the President. The Council made three recommendations:

1. The University shall take appropriate action to terminate the TALX contract;
2. The University shall take responsibility for purging all employee information from the TALX databases; and
3. The Office of General Counsel shall review its opinion that the University has the authority to disclose employee information without the consent of its employees.

As a result, the TALX contract was terminated. We were made the following promises: in similar cases in the future, faculty will be consulted and any similar program will be on a strictly opt-in basis.

In October 2016, I was surprised to find out that UC had subsequently outsourced our data to TALX's successor, Equifax Workforce Solutions. To the best of my knowledge, there wasn't

---

[2] There is no mention of Equifax on the UCPath site.

[3] You may ask, can't anyone get access to our salary information, anyway, through public sites like the Sacramento Bee? Can't anyone just harvest that data? Public sites give only our annual salary, and only with more than a year delay. Our payroll data is delivered monthly or bi-weekly to Workforce Solutions and includes length of employment, and most importantly, unique IDs, like the SSN, that allow Equifax to merge our data with other records.

even a public announcement that this would happen. When I inquired about the promised consultation I was informed that:

"The UCPath Center Leadership met with several groups at UC Office of the President to explain The Work Number process and gain approval. On October 28, 2014 UCPath Center Leaders met with Vice Provosts of Academic Personnel including Vice Provost Carlson and on November 14, 2014 they met with Academic Senate Faculty Welfare Committee meeting chaired by [XXX] from UC San Diego. Both of these groups reviewed and approved the program for the University of California."

The "consultation" described above took place in 2014, while the first contract was signed in 2013 and, as I found out, at least two campuses, UC Riverside and UC San Diego, already had their own agreements with Equifax and had been already delivering data as early June 1, 2012.

As for the "strictly opt-in" promise, that one was not kept either. Currently, even opting out is a major challenge. Last year, I was promised that an easy way of opting out would be implemented soon. This has yet to happen.

Below I will expand on the three main concerns about outsourcing our payroll data to Equifax, and why we need to worry about our ability to control our data and our data privacy.

Weak Data Security

The first reason why payroll outsourcing is harmful is that Equifax has a terrible history of data breaches. A few examples:

> In 2016, tax information of 431,000 employees of the grocery chain Kroger was stolen from Equifax.
>
> The same year, the data of 600 Stanford University and 150 Northwestern University employees was taken from Equifax.
>
> In early 2017, hackers broke into Workforce Solutions and took tax information of 750 employees of the University of Louisville, Kentucky, which resulted in over 70 fraudulent tax claims.
>
> Between April 17, 2016 and March 29, 2017, several breaches compromised the records of employees of defense contractor giant Northrop Grumman; staffing firm Allegis Group, building materials manufacturer Saint-Gobain Corp., and Erickson Living, an operator and developer of retirement communities.
>
> In March, 2017, Equifax was notified by Apache, a software developer, that its Apache Struts web application, used by Equifax, had a security bug and was offered a patch. Equifax failed to install it. In mid-May, hackers broke into Equifax and had access to

client data until July 29, 2017. [4] The breach was reported only on September 7, 2017.[5] The count of compromised records as of March 3, 2018, stands at 147.9 million in the US alone. The last 2.4 million records, that includes among other things driver's license numbers, were just reported officially on March 1, 2018.[6]

We still do not know the true extent of the damage. What we have found out so far was the product of intense Senate investigations. Senator Elizabeth Warren wrote: "I spent 5 months investigating the Equifax breach and found the company failed to disclose the full extent of the hack. Today, Equifax acknowledged that 2.4 million more people were affected than initially reported and that driver's license information was also stolen. Equifax can't be trusted. Their mistakes allowed the breach to happen, their response has been a failure, and they still can't level with the public."[7]

Despite these breaches, in the 2017 proxy statement attached to its 2016 Annual Report, Equifax justifies bonuses to its CEO, Richard Smith and CFO John Gamble, among other things, by citing their outstanding records in data security. This is after a year of serious breaches, written just a few days after the Apache notification.

How much confidence can we have in what Equifax tells us about its data security? Not much.

Poor Service

Credit registries like Equifax have had a long history of data problems. External research on bad data in credit bureaus focused on credit records, as data aggregation from other sources is a relatively new phenomenon. The Federal Trade Commission has conducted five reports between 2004 and 2012 on the accuracy of credit histories and found various discrepancies. In its latest, 2012 study, the Federal Trade Commission found that 21 percent of consumers had identified errors that have subsequently resulted in a change in their record.[8]

The three credit bureaus are notoriously recalcitrant when it comes to consumer complaints. Most of their customer service is outsourced to India, Chile and the Philippines, and requests for corrections may take years. The bureaus are better off settling court cases with the most

---

[4] There is well-founded suspicion of insider trading. We know that Equifax Chief Financial Officer John Gamble sold shares worth nearly $950,000 on August 1. Joseph Loughran, Equifax's president for U.S. information solutions, sold shares on the open market worth about $584,000 on August 1 as well. And Rodolfo Ploder, president of Workforce Solutions, sold stock for more than $250,000 on August 2. At that time, the share price was $145. After the data breach announcement, the share price plummeted to $92. Currently, it is under $120. In November, Equifax's board cleared the executives of all charges of insider trading. Still, in mid-March, 2018, Jun Ying, Equifax's former ex-chief information officer, was criminally charged for allegedly selling almost $1 million worth of shares before the company's announcement last year that it had suffered a massive data breach.

[5] The delay gave hackers plenty of time to take advantage of their data.

[6] It is unclear, why and how Equifax has driver's license data.

[7] Equifax's first response was to try to sell a credit monitoring service to people whose data was compromised but it soon backed down, its CEO apologized, and later resigned. Perversely, even with offering free credit freeze to most customers, the three credit bureaus netted $1.4 billion from charging for freezing, unfreezing and re-freezing accounts.

[8] Thirteen percent had a change that affected their credit score and five percent of consumers moved into a lower risk tier in a way that would make a significant difference in future borrowing.

persistent complainers than committing to investigating thoroughly every complaint brought to them.

Equifax receives the most complaints at the CFPB. Before its massive breach, between February and April 2016, it led the pack with a monthly average of 1,301 (followed by the other two big credit registries: Experian (1,178), and TransUnion (1,000)).

There are many journalistic treatments of the horrific customer service Equifax and the other two registries provide. One excellent piece is by John Oliver.

In brief, if you find an error in your Equifax file, your ability to correct it is very limited.

Data Aggregation

Since the late 2000s Equifax has embarked on a project of data aggregation. The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999 (the one that replaced Glass-Steagall) removed the obstacles that prevented companies from sharing data among subsidiaries they own. As long as two companies belong to the same holding, they can exchange information.

As a result, companies began to aggregate data by acquiring other, data rich companies. Initially, Equifax planned to use payroll data only to "beef up" so called "thin files." Thin files are credit records with little or no data for an individual. Yet, there is no reason for Equifax to stop at thin files and not use payroll data where it is available for all files in calculating the single number that summarizes one's credit record, called the credit (or FICO) score. And Equifax, indeed, did not stop there. It also purchased Discovery Solutions, a tax data specialist company and IXI Corp, collecting wealth related information. In two company videos, Equifax explains how they use payroll, tax and wealth data to create their new product: Decision 360™.

Decision 360 ™, The True 360° Consumer View™, "draws from a wealth of unique data sources and insights that include:

• Exclusive access to more than $10 trillion in investable asset data [IXI].
• 195+ million active employment records from more than 2,000 U.S. employers [TALX].
• Tax transcript information, delivered in 24-48 hours, verified directly from the IRS [Discover Source/TALX].
• SSN verification based on searches of more than 15 billion public/private databases, and authenticated by the Social Security Administration.
• An extensive credit reporting database of more than 250 million consumer records [Equifax's original credit registry]."

There is a lot more to come. In 2016, at a financial conference, Rick Smith, then CEO of Equifax, according to the New York Times, "described a new system that searched four billion public tweets for keywords like "car" and "automotive lease." It paired the tweets with a person's Equifax credit file. In real time, the credit bureau could identify potential buyers and provide its customer, a company selling car leases, with everything it wanted to know about those people."

Why you should worry

It doesn't take much explanation why one should worry about *weak data security* that may lead to identity theft. You may wonder, though, why it is the individuals who must pay the entire price. If your data is stolen and used to open a new loan account or to file for false tax returns, why is it not the lender or the IRS who should be responsible for not properly checking the identity? Why is the burden of proof on the victim?

UC administration argues, and so does Equifax, that our data is more secure with a company specializing in data management and protection than with UC. This is a strange argument that assumes that data is like gold: once you move it from your cupboard to a bank vault, you are more secure. The fact is that our data remains with UC, even if it is handed over to Equifax. Giving it to Equifax only provides another opportunity for hacking. Hacking Equifax may be harder than hacking UC, but it is much more lucrative, as one hack can yield many more records. Outsourcing further reduces safety.

Why one should care about *poor customer service* is also not hard to see. Correcting errors, settling disputes are daunting with a company unaccountable to the people whose data it processes.

Why one should be concerned about *data aggregation* is perhaps less obvious. UC's contract with Equifax does not permit the sale of our payroll data to third parties,[9] but it doesn't prohibit the transfer of data within Equifax, which is why Equifax can merge payroll with credit records.

Data aggregation tightly couples various forms of social disadvantage. Suppose you lose your job. Merging payroll data with your credit history results in an immediate downgrading of your credit profile and your credit score will drop. As a result, just when you are most vulnerable, your access to credit becomes more difficult and expensive, making default more likely. Worse yet, credit scores are also used by insurance companies setting car insurance premiums, by landlords in negotiating and granting rental applications and by the majority of private companies in hiring as part of their background checks. Higher car premiums, worse rental conditions and inability to find your next job will all affect your score adversely. Individuals can be thrust into a downward spiral. At a societal level, this amplifies inequalities. (I explain this in more detail in this publication.)

Finally, Equifax may expand its business into new realms. In the past, Equifax was found selling TWN data to debt collection agencies but that is not illegal. Were Equifax to launch its own debt collection business, it could move payroll data – even ours -- not just legally but also invisibly to exploit "data synergies."

As big data inevitably proliferates in the world, the rules of the game are still evolving. Our actions now will decide how much control we keep over our information. UC walked into a contract, probably to save a few dollars, squandering our control over our own data. UC is the

[9] There is no way we can know if Equifax complies with this prohibition.

largest employer in the largest state. It should respect our data privacy and should set a national example.

Additional links:

Watch Dann Adams, President of TALX explains data aggregation and the role of TALX in Equifax's effort. (Needs Adobe Flash Player)

https://www.equifax.com/d360/assets/

Watch Janet Ford, Senior Vice President for The Work Number explain Decision 360. (Needs Adobe Flash Player)

https://www.equifax.com/d360/unique/

A recent article on why the New York Times pulled out of its contract with Equifax and why other employers should follow suit.

https://www.nytimes.com/2018/01/26/your-money/equifax-breach.html

Equifax CEO Richard Smith testifying in front of the U.S. Senate Banking Panel on October 2017

https://www.c-span.org/video/?434469-1/equifax-ceo-testifies-senate-banking-panel

And some of the highlights

https://www.wired.com/story/equifax-ceo-congress-testimony/