WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum regarding the proposed consent order in The Matter of Ceridian Corporation, FTC File No. 102 3160

Federal Trade Commission
Office of the Secretary
Room H-135
600 Pennsylvania Avenue, NW
Washington DC 20580

May 27, 2011

Re: In the Matter of Ceridian Corporation, FTC File No. 102 3160, 76 Federal Register 26729 (May 9, 2011), http://www.gpo.gov/fdsys/pkg/FR-2011-05-09/pdf/2011-11183.pdf

The World Privacy Forum offers comments on the proposed consent order, In the Matter of Ceridian Corporation, FTC File No. 102 3160. The World Privacy Forum is a non-profit, non-partisan public interest research group that focuses on consumer education as well as analysis and research of privacy issues, including issues relating to health care privacy, technology, and online/offline data privacy. More information on our work may be found at http://www.worldprivacyforum.org.

We have nothing to say in defense of the actions or statements of Ceridian. Our comments focus on the choices made by the Commission in pursuing this matter, in setting out the facts of the case, and in selecting the basis for this action. We want to be clear that we support the FTC's many actions in support of privacy, and we appreciate the Commission's efforts on behalf of consumers. However, we are seeing the outlines of some consistent patterns in the Commission's enforcement efforts, and we have some suggestions and comments regarding potential improvements in these patterns. Our comments below discuss these issues in more detail.

1. Lack of transparency in the complaint process

To begin, we observe that the Commission's complaint process is a black box. The FTC encourages consumers to file complaints, but yet the public has no idea which complaints the Commission has chosen to investigate, which complaint are open, which complaints are closed, or which complaints have been effectively ignored. As a result, the public and the industry have no sense of what are the Commission's interests or priorities. There are only vague statements from Commission members and staff and the occasional consent decree that appears from time to time.

The public and the industry have no idea what might come next or when. Commission actions on privacy are, effectively, random with respect to time and target, especially when viewed from outside. Each company subject to the Commission's jurisdiction knows well that Commission resources are limited and that the chances that the Commission will actually target any individual company for deceptive practices are quite small. Our concern here is that as a result, the pressure that the Commission seeks to exert on industry is effectively dissipated.

2. Why did the Commission choose to pursue this case? What and where are the facts for the public?

The documents released in connection with the proposed consent decree shed no light on why the Commission chose this case out of all the cases that it might have brought. There simply are not enough facts to judge the reasons for the Commission's actions.

Paragraph 9 of the complaint discloses how many individuals were affected by the breach and includes some information about what types of information was obtained. But the complaint says obscurely including, *in some instances*, bank account numbers, Social Security Numbers, and dates of birth. We have numerous questions about the facts here. Were bank account numbers obtained on two or on twenty thousand individuals? In and of itself, that number would not be important. However, we believe that the public is entitled to know more facts in order to assess the decision of the Commission to use its scarce investigative resources to bring this action.

We would also like to know if any of the individuals whose records were obtained suffer monetary losses? Were any of the victims obliged to spend significant time and effort to clear up the consequences of the breach on their bank accounts? Did anyone actually become a victim of identity theft as a result of the breach? These facts are material to any evaluation of the Commission's choice to pursue this case. Did the Commission acquire the answers to these questions?

We also wonder why was this case selected while other similar cases were ignored? The Commission owes the public an explanation, yet the documents released shed little light. The Privacy Rights Clearinghouse reports that there have been more than 2000 breaches in recent years. Why and how does the Commission select a handful of those breaches to pursue? The public has no idea. Was the Ceridian breach more significant than the hundreds of other reported breaches that took place that same year? Was there a pattern of insufficient security and other breaches at Ceridian that warranted the action? Was the number of affected individuals particularly large? The complaint says that at least 27,673 were affected. This is a sizeable number, but it is dwarfed by the numbers in many other security breach cases.

We have complained in previous cases that the Commission fails to tell the public enough facts in the few cases that it chooses to bring. We understand compromises are part of the process of arriving at a consent decree with the business entity in question, but it is never appropriate to compromise on the public's right to know what the Commission does and why. Even if certain facts are embarrassing for the business in question, the public has a right to know what those facts are.

The Commission's pervasive secrecy in its investigative priorities and its complaint handling invites speculation. Was this case brought because there was something of particular significance in the facts of this case? Was this case brought because it was as "easy" win for the Commission? Was it brought to improve the numbers for the Commission's budget request? We have no basis to speculate that the case was selected for political or other inappropriate reasons, but the truth is that we do not know. The Commission has not indicated what its priorities are or what it wants to accomplish in filing complaints. The policy of the Commission should be to allow the public to be able to fairly evaluate its activities and to hold it accountable for its decisions.

3. The Commission's pursuit of cases based on deceptive practices accomplishes little to provide guidance to companies or to consumers

We recognize that if a company says one thing and does another, the Commission's jurisdiction over deceptive trade practices may be invoked to sanction the company. It is well established in case after case that deceptive trade practices are illegal. We understand this, and we believe that generally most companies understand this.

We suspect that given enough resources, the Commission could pursue thousands or hundreds of thousands of deception cases on Internet cases alone. The real problem with deception cases is that each case teaches the exact same lesson: deceptive trade practices are illegal. Consumers learn nothing, and business learns mostly to make promises using more carefully nuanced language. The result is vaguer language in privacy policies and promises without substance. In the end, consumers are worse off, and the Commission's ability to pursue deception cases diminishes because corporate lawyers massage privacy policy statements to remove overt statements and implied promises that might be used to hold their clients accountable.

We choose not to dissect the specific words used by Ceridian in its privacy statement. We think that the words from the Commission's complaint warrant review, and we reproduce two paragraphs here.

> 10. Through the means described in Paragraphs 6 and 7, respondent represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect personal information against unauthorized access.
>
> 11. In truth and in fact, respondent did not implement reasonable and appropriate measures to protect personal information against unauthorized access. Therefore, the representations set forth in Paragraphs 6 and 7 were, and are, false or misleading.

We focus on the words *expressly or by implication*. We understand express representations and assume arguendo that there may have been express representations in this case that were violated, but we wonder just how strong that case is. We are at a loss to understand why or even how the Commission can base a case for deceptive practices on the *implications* of a company's

privacy policy. How much does the Commission propose to dissect privacy policies to extract all of the implications in those policies and then hold companies to them?

Research shows that consumers overvalue the mere fact that a website has a privacy policy, and that many consumers assume that a website with a policy has strong default rules to protect personal privacy, even when the policy itself makes no such promise express of implied.[1] We would be happy to applaud an action by the Commission holding that the presence of any privacy policy regardless of its content implies strict limits on disclosure. That is what much of the public perceives from the presence of a privacy policy statement or link. We would welcome a strong, clear conclusion from the Commission if we thought that the courts would allow it under current law.

Nevertheless, we wonder just how far the Commission's power extends to holding companies to the *implications* of their statements and not just to the content of the statements. In advertising matters, we note that the Commission does not take enforcement actions against some express statements (puffery) that ordinary consumers do not take seriously. Can the Commission really hold companies to the *implications* of privacy statements that are rarely read by any consumer?

In basing this case, we wonder if the Commission was uncertain if Ceridian's express promises were too hedged to support the action on that basis alone. Is a lesson from this case that lawyers should start writing disclaimers for implied promises?

In short, we wonder if actions based on *implications* will benefit consumers in the long run or guide business in the short term.

4. The Commission should bring more cases that rely on unfair practices

Because we believe that there is little to be learned from deceptive practice cases, we ask the Commission to bring cases relying on the law banning unfair trade practices. What is needed in these cases is for the Commission to state positively and with more specificity ***what constitutes unfair conduct***. In the security area, there are plenty of statements of public policy, industry adopted standards, and declarations of best practices so that the Commission should be able to base an unfairness case on clearly established and generally recognized principles. There is no need to for the Commission to create security standards out of whole cloth.

We observe that the Ceridian case did include some language about unfairness. The complaint provided in paragraph 12:

> As set forth in Paragraph 8, respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information. Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or

[1] See, e.g., Chris Jay Hoofnagle & Jennifer King, *What Californians Understand about Privacy Online* (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130.

> competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

The problem is that this use of unfairness is much too small a step to be valuable. The Commission's statement about unfairness in this case is too vague and too general to offer any real guidance to anyone. What is a *reasonable and appropriate measure*? The complaint does not say. The unfairness part of the complaint is really no more than one sentence. What must a company do to avoid a finding of unfairness? Is it unfair simply to suffer from a security breach?

We would like to see the Commission make a specific determination in a security case that it is unfair for a website processing personal information:

1) not to have a security policy;
2) not to conduct a risk analysis as part of its security policy;
3) not to employ sufficient encryption to protect personally identifiable information;
4) not to use password protection to limit access to data; and
5) not to require passwords to be changed routinely.

We offer this list as an example of the type of conclusions that the Commission could make in reaching a conclusion that a company's security practices are unfair. We realize that a complete list of security standards would be longer and more nuanced.

If the Commission were to use its existing authority to define in more detail what constitutes unfairness, it would go a long way to establish clearer standards for companies and produce better results for consumers. The specifics in the consent decrees in these cases do not accomplish these objectives. All that we know is that the company prosecuted did something to step over the line that separates acceptable from unacceptable conduct. However, we have no idea where the Commission draws that line.

Use of the Commission's unfairness jurisdiction has the ability to clarify the obligations of those who process personally identifiable information on websites and otherwise. There is little to be gained by pursuing deceptive trade practices one by one.

The World Privacy Forum believes that the Commission can do a better job protecting consumers and guiding business by making clearer, more transparent, and more effective use of its unfairness jurisdiction in privacy and security cases. We ask that the Commission decline to accept the Ceridian consent decree and that it start again by focusing principally on the unfair trade practices that are at the center of the case. We believe this will be a positive shift and will benefit consumers, and ultimately, the companies relying on FTC guidance.

Respectfully submitted,

s/o

Pam Dixon

Executive Director, World Privacy Forum
www.worldprivacyforum.org