**Before the**
**Federal Trade Commission**
**Washington, DC 20580**

| | |
|---|---|
| **In the Matter of** | **)** |
| | **)** |
| **Google, Inc. and** | **)** |
| **Cloud Computing Services** | **)** |
| **_____** | **)** |

**Complaint and Request for Injunction, Request for Investigation and for Other Relief**

## SUMMARY OF COMPLAINT

1. This complaint concerns privacy and security risks associated with the provision of "Cloud Computing Services" by Google, Inc. to American consumers, businesses, and federal agencies of the United States government. Recent reports indicate that Google does not adequately safeguard the confidential information that it obtains. Given the previous opinions of the Federal Trade Commission regarding the obligation of service providers to ensure security, EPIC hereby petitions the Federal Trade Commission to open an investigation into Google's Cloud Computing Services, to determine the adequacy of the privacy and security safeguards, to assess the representations made by the firm regarding these services, to determine whether the firm has engaged in unfair and/or deceptive trade practices, and to take any such measures as are necessary, including to enjoin Google from offering such services until safeguards are verifiably established. Such action by the Commission is necessary to ensure the safety and security of information submitted to Google by American consumers, American businesses, and American federal agencies.

## PARTIES

1. The Electronic Privacy Information Center ("EPIC") is a public interest research organization incorporated in Washington, DC. EPIC's activities include the review of government and private sector policies and practices to determine their impact on the privacy interests of the American public. Among its other activities, EPIC initiated the complaint to the FTC regarding Microsoft Passport in which the Commission subsequently required Microsoft to implement a comprehensive information security program for

Passport and similar services.[1] EPIC also filed the complaint with the Commission regarding databroker ChoicePoint, Inc.[2] In that matter, the Commission determined that ChoicePoint's failure to employ reasonable security policies compromised the sensitive personal data of consumers, and assessed fines of $15 m.[3] Further, EPIC brought the complaint to the Federal Trade Commission regarding the need to establish privacy safeguards as a condition of the Google-Doubleclick merger.[4] Although the Commission failed to act in that matter, a subsequent review by the Department of Justice in a similar matter made clear that such a consolidation of Internet advertisers would have led to monopoly concentration and would have been against the public interest.[5]

2. Google, Inc. ("Google") was founded in 1998 and is based in Mountain View, California. Google's headquarters are located at 1600 Amphitheatre Parkway, Mountain View, CA 94043. At all times material to this complaint, Google's

---

[1] In the Matter of Microsoft Corporation File No. 012 3240, Docket No. C-4069 (Aug. 2002), *available at* ttp://www.ftc.gov/os/caselist/0123240/0123240.shtm. See also, Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microsoft.shtm.

[2] *See* EPIC, *EPIC Choicepoint Page*, http://epic.org/privacy/choicepoint/.

[3] U.S. Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006, available at: http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

[4] In the Matter of Google, Inc. and DoubleClick, Inc., Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Sept. 20, 2007), *available at* http://epic.org/privacy/ftc/google/epic_complaint.pdf; Privacy? Proposed Google/DoubleClick Deal, http://epic.org/privacy/ftc/google/ (last visited Mar. 16 2009).

[5] "Google Won't Pursue Yahoo Ad Deal," N.Y. Times, Nov. 5, 2008 ("The Justice Department notified Google and Yahoo early Wednesday that it was planning to file suit to block the deal, which called for Google to place ads alongside some of Yahoo's search results."), *available at* http://www.nytimes.com/2008/11/06/technology/internet/06google.html*; see also* Dep't of Justice, "Yahoo! Inc. and Google Inc. Abandon Their Advertising Agreement -Resolves Justice Department's Antitrust Concerns, Competition Is Preserved in Markets for Internet Search Advertising," Nov. 5, 2008, *available at* http://www.usdoj.gov/opa/pr/2008/November/08-at-981.html.

course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

## THE IMPORTANCE OF PRIVACY PROTECTION

3. The right of privacy is a personal and fundamental right in the United States. The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.

4. The excessive collection of personal data in the United States coupled with inadequate legal and technological protection have led to a dramatic increase in the crime of identity theft.[6]

5. Cloud Computing Services are rapidly becoming an integral part of the United States economy, with implications for business development, security, and privacy. A March 2009 study expects corporate IT spending on cloud services to grow almost threefold, reaching US$42 billion, by 2012.[7]

6. The Federal Trade Commission has a statutory obligation to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where companies have engaged in unfair and/or deceptive trade practices.

## STATEMENT OF FACTS

*"Cloud Computing Services" Defined*

7. "Cloud Computing Services" involve "a software and server framework (usually based on virtualization)" that uses "many servers for a single

---

[6] Fed. Trade Comm'n, "FTC Releases List of Top Consumer Fraud Complaints in 2008"(Feb. 26, 2009) (The list, contained in the publication "Consumer Sentinel Network Data Book for January-December 2008," showed that for the ninth year in a row, identity theft is the number one consumer complaint, with 313,982 complaints received) *available at* http://www.ftc.gov/opa/2009/02/2008cmpts.shtm. The recent FTC report also indicates a particular risk to individuals ages 20-29, *i.e.* the Internet users who are becoming most dependent on new cloud based services.

[7] "IDC Says Cloud Computing Is More Than Just Hype; Worldwide IT Spending On Cloud Services Expected To Reach US$42 Billion By 2012," Press Release, Mar. 6, 2009 *available at* http://www.idc.com/getdoc.jsp?containerId=prMY21726709.

software-as-a-service style application or to host many such applications on a few servers."[8]

8. Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices.[9] This model of service delivery is in contrast to an architecture in which data and applications typically reside on servers or computers within the control of the end-user.

9. Some Cloud Computing Services use encryption, by default, to "respect individual privacy" and "provide users with the ability to fully control and customize their online experience."[10] One firm has stated that it is a "key principle" that "users own their data, and have complete control over its use. Users need to explicitly enable third parties to access their data."[11]

*American Consumers, Educators, and Government Employees Are Increasingly Using Cloud Computing Services*

10. As of September 2008, 69 percent of Americans were using webmail services, storing data online, or otherwise using software programs such as word processing applications whose functionality is located on the web.[12]

11. According to a report of the Pew Internet and American Life Project, an overwhelming majority of users of Cloud Computing Services expressed serious concern about the possibility that a service provider would disclose their data to others:[13]

    - 90% of cloud application users say they would be very concerned if the company at which their data were stored sold it to another party.

---

[8] "Perspectives on Cloud Computing and Standards," NIST, Information Technology Laboratory, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf (last visited Mar. 11, 2009).

[9] "Cloud Computing Gains in Currency," Internet and American Life Project, (Sep. 12, 2008), *available at* http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency. *See also* Cloud computing, Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing (last visited Mar. 16, 2009).

[10] Introducing Weave, Mozilla, Dec. 12, 2007, available at http://labs.mozilla.com/2007/12/introducing-weave.

[11] Overview of OAuth for Weave, https://wiki.mozilla.org/Labs/Weave/OAuth (last visited Mar. 16, 2009).

[12] *Id*.

[13] "Cloud Computing Gains in Currency," *supra* note 9.

- 80% say they would be very concerned if companies used their photos or other data in marketing campaigns.

- 68% of users of at least one of the six cloud applications say they would be very concerned if companies who provided these services analyzed their information and then displayed ads to them based on their actions.

12. A recent survey from TRUSTe underscores ongoing concern about Internet-based services, with 35% of users responding that their privacy has been invaded or violated in the last year due to information they provided via the Internet.[14]

*Google's Cloud Computing Services - Representations*

13. Google currently provides an extensive array of Cloud Computing Services, including email ("Gmail"), [15] online document storage and editing ("Google Docs"),[16] integrated desktop and internet search ("Google Desktop"),[17] online photo storage ("Picasa Web Albums"),[18] and scheduling programs ("Google Calendar"). [19]

14. In September 2008, comScore Media Metrix reported that 26 million consumers used Google's Gmail Cloud Computing Services.[20]

15. In November 2008, 4.4 million consumers used the Google Docs Cloud Computer Service.[21]

16. The number of consumers using Google Docs more than doubled in 2008, increasing 156 percent.[22]

17. Critical to the architecture of every single Google Cloud Computing Service is that the customer's data resides on a Google server, *i.e.* a computer-based

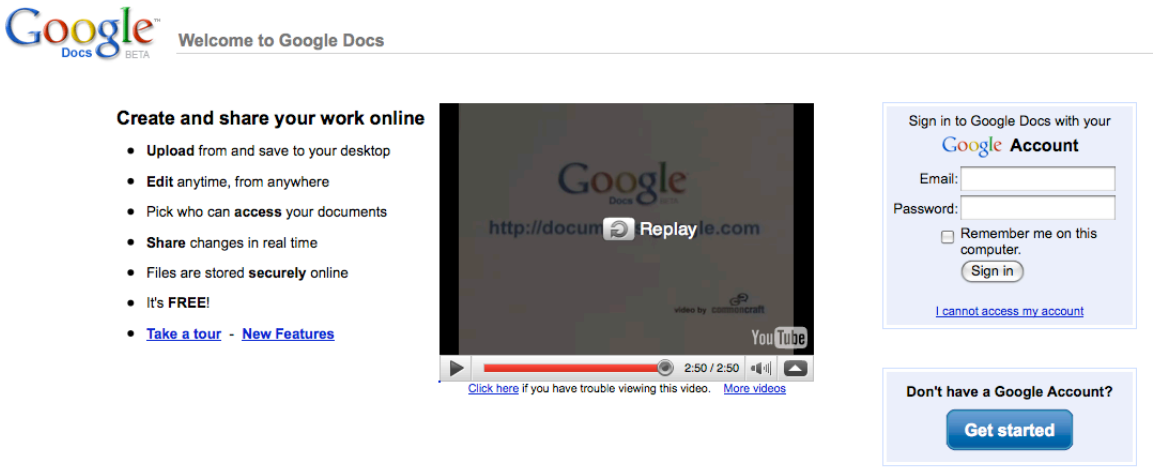
---

[14] Behavioral Advertising Survey, TRUSTe, Mar. 4, 2009 *available at* http://www.truste.org/about/press_release/03_04_09.php.
[15] Gmail, http://mail.google.com (last visited Mar. 17, 2009).
[16] Google Docs, http://docs.google.com (last visited Mar. 17, 2009).
[17] Google Desktop, http://desktop.google.com (last visited Mar. 17, 2009).
[18] Picasa Web Albums, http://picasaweb.google.com (last visited Mar. 17, 2009).
[19] Google Calendar, http://www.google.com/calendar (last visited Mar. 17, 2009).
[20] Saul Hansell, AOL's Luddites Love Their E-Mail More Than Google's Geeks, N.Y. Times, Sept. 12, 2008 *available at* http://bits.blogs.nytimes.com/2008/09/12/aols-luddites-love-their-e-mail-more-than-googles-geeks.
[21] "Happy 2nd Anniversary, Google Docs & Spreadsheets," Nov. 13, 2008 *available at* http://blog.compete.com/2008/11/13/google-docs-spreadsheets-microsoft-office.
[22] *Id*.

information retrieval system under the control of Google – not the customer or end-user.

18. The permanent transfer of the user's data, from devices and servers within the control of the user, to Google has profound implications for privacy and security.[23]

19. Google routinely represents to consumers that documents stored on Google servers are secure. For example, the homepage for Google Docs states "Files are stored **securely** online" (emphasis in the original) and the accompanying video provides further assurances of the security of the Google Cloud Computing Service.[24]



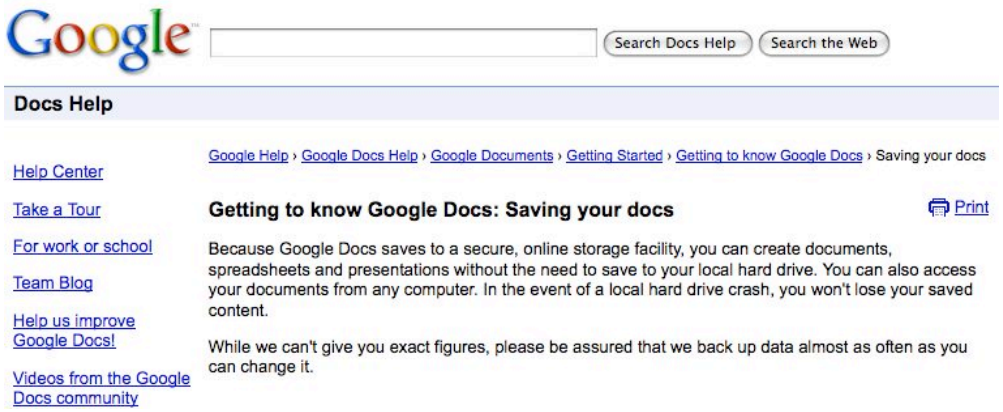

20. Google also explicitly assures consumers that "Google Docs saves to a secure, online storage facility . . . without the need to save to your local hard drive."[25]

---

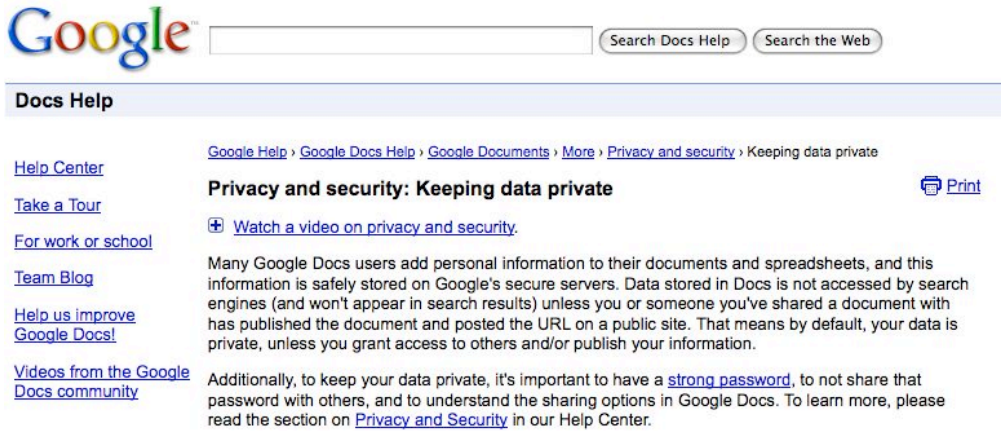
[23] *See, e.g.,* World Privacy Forum, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," Feb. 26, 2009, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

[24] "Welcome to Google Docs," https://docs.google.com/ (last visited Mar. 8, 2009).

[25] "Getting to know Google Docs: Saving your docs," http://docs.google.com/support/bin/answer.py?answer=44665&topic=15119 (last visited Mar. 11, 2009); *see also* "Getting to know Google Docs: Saving your presentation," http://docs.google.com/support/bin/answer.py?hl=en&answer=69074 (last visited Mar. 11, 2009).




21. Google encourages users to "add personal information to their documents and spreadsheets," and represents to consumers that "this information is safely stored on Google's secure servers." Google states that "your data is private, unless you grant access to others and/or publish your information."[26]

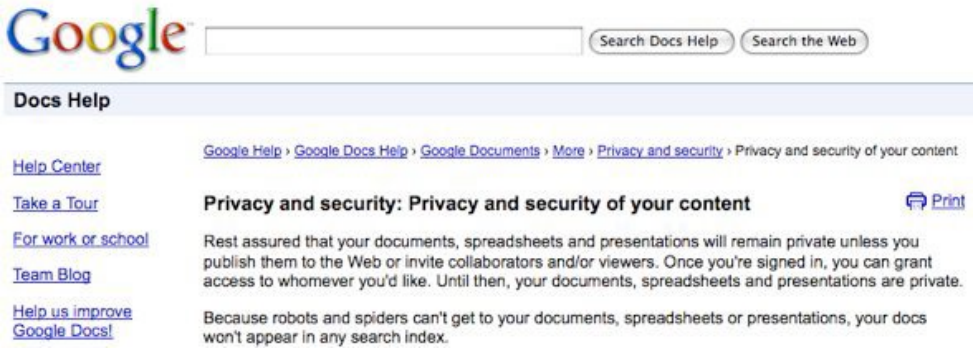



22. Google represents to consumers, "Rest assured that your documents, spreadsheets and presentations will remain private unless you publish them to the Web or invite collaborators and/or viewers."[27]

---

[26] "Privacy and security: Keeping data private," http://docs.google.com/support/bin/answer.py?hl=en&answer=87149 (last visited Mar. 11, 2009).

[27] "Privacy and security: Privacy and security of your content," http://docs.google.com/support/bin/answer.py?answer=37615&ctx=sibling (last visited Mar. 11, 2009)




23. However, Google's Terms of Service explicitly disavow any warranty or any liability for harm that might result from Google's negligence, recklessness, mal intent, or even purposeful disregard of existing legal obligations to protect the privacy and security of user data.[28]

*Google's Cloud Computing Services – Known Flaws*

24. On March 7, 2009, Google disclosed user-generated documents saved on its Google Docs Cloud Computing Service to users of the service who lacked permission to view the files. (the "Google Docs Data Breach")[29] This is just one of many example of known flaws with Google's Cloud Computing Services. For example:

    - In January 2005, researchers identified several security flaws in Google's Gmail service. The flaws allowed theft of "usernames and passwords for the 'Google Accounts' centralised log-in service" and enabled outsiders to "snoop on users' email."[30]

    - In December 2005, researchers discovered a vulnerability in Google Desktop and the Internet Explorer web browser.[31] The security flaw exposed Google users' personal data to malicious internet sites.[32]

---

[28] Google Terms of Service, ("14. Exclusion of Warranties," "15. Limitation of Liability" http://www.google.com/accounts/TOS?hl=en

[29] "On Yesterday's email," Mar. 7, 2009, *available at* http://googledocs.blogspot.com/2009/03/on-yesterdays-email.html; *see also* "Google Discloses Privacy Glitch," The Wall Street Journal, Mar. 8, 2009, *available at* http://blogs.wsj.com/digits/2009/03/08/1214.

[30] John Leyden, Google plugs brace of GMail security flaws, The Register, Jan. 17, 2005 *available at* http://www.theregister.co.uk/2005/01/17/google_security_bugs.

[31] Google Desktop Exposed: Exploiting an Internet Explorer Vulnerability to Phish User Information, Matan Gillon, Nov. 30, 2005 *available at* http://www.hacker.co.il/security/ie/css_import.html; *see also* Andrew Orlowski, Phishing with Google Desktop, The Register, Dec. 3, 2005 *available at* http://www.theregister.co.uk/2005/12/03/google_desktop_vuln.

- In January 2007, security experts identified another security flaw in Google Desktop. The vulnerability "could enable a malicious individual to achieve not only remote, persistent access to sensitive data, but in some conditions full system control."[33]

25. Computer security expert Greg Conti observes that data breaches at Google are particularly problematic relative to other Cloud Computing Services providers: "Google is an even *bigger* target because of the amount of data it has."[34] (emphasis in the original).

26. Furthermore, users face risks posed by the very nature of Cloud Computing Services:

> By placing applications, and their data files, on centralized servers, we lose control of our data. Critical information that was once safely stored on our personal computers now resides on the servers of online companies. . . . With [Cloud Computing Services], we could find both access to the application and our data at risk by placing both in the hands of a third party.[35]

## THE FTC'S AUTHORITY TO REGULATE UNFAIR AND DECEPTIVE TRADE PRACTICES

27. Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), prohibits unfair or deceptive acts or practices in or affecting commerce.

28. The Federal Trade Commission ("FTC") generally identifies three factors that support a finding of unfairness: whether the practice injures consumers, whether it violates established public policy, and whether it is unethical or unscrupulous.[36] A practice is "unfair" if: 1) it causes substantial injury to

---

[32] *Id*.

[33] Watchfire Discovers Google Desktop Vulnerability That Hackers Could Exploit to Gain Full System Control, Press Release, Feb. 21, 2007 *available at* http://web.archive.org/web/20070223064417/http://www.watchfire.com/news/releases/02-21-07.aspx; see also Yair Amit, Danny Allan, and Adi Sharabani, Overtaking Google Desktop, 2007 *available at* http://web.archive.org/web/20070223064417/http://download.watchfire.com/whitepapers/Overtaking-Google-Desktop.pdf.

[34] GREG CONTI, GOOGLING SECURITY at 19 (2009).

[35] *Id*. at 15.

[36] Fed. Trade Comm'n Policy Statement on Unfairness (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

consumers; b) the harm is not outweighed by any countervailing benefits; and c) the harm is not reasonably avoidable.[37]

29. Google's inadequate security practices, and the resultant Google Docs Data Breach, caused substantial injury to consumers, without any countervailing benefits.

30. The harm was reasonably avoidable, in that the damage could have been avoided or mitigated by the adoption of commonsense security practices, including the storage of personal data in encrypted form, rather than in clear text.

31. Deception occurs under Section 5 if there is a material representation, omission, or practice that is likely to mislead reasonable consumers.[38] The FTC Policy Statement on Deception states that the Commission analyzes deceptive business practices under the following rubric:

> a) There must be a representation, omission or practice that is likely to mislead the consumer. This includes the "use of bait and switch techniques."[39]
>
> b) The practice is examined from the perspective of a reasonable person in the circumstances. If the practice "is directed primarily to a particular group," such as Internet users, "the Commission examines reasonableness from the perspective of that group."[40]
>
> c) The representation, omission or practice must be a material one, *i.e.* it is likely to affect the consumer's conduct or decision regarding the product or service.[41]

32. Google made material representations that misled consumers regarding its security practices, and users reasonably relied on Google's promises.

33. As demonstrated by the Google Docs Data Breach, Google's material representations were deceptive.

## PREVIOUS FTC DATA SECURITY ACTIONS

[37] *Orkin Exterminating Company, Inc. v. FTC*, 849 F.2d 1354, 1364 (11th Cir. 1988).
[38] Fed. Trade Comm'n, Policy Statement on Deception, Oct. 14, 1983, *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.
[39] *Id*.
[40] *Id*.
[41] *Id*.

34. Under its Section 5 authority, the FTC has "brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information."[42]

35. The Commission has also "used its unfairness authority to challenge information practices that cause substantial consumer injury."[43]

36. On March 27, 2008, FTC Chairman Deborah Platt Majoras stated:

> By now, the message should be clear: companies that collect sensitive consumer information have a responsibility to keep it secure … the FTC has charged companies with security deficiencies in protecting sensitive consumer information [on more than 20 occasions]. Information security is a priority for the FTC, as it should be for every business in America.[44]

*The Choicepoint Settlement*

37. In 2005, the Commission determined that ChoicePoint's failure to employ reasonable security policies compromised the sensitive personal data of more than 163,000 consumers.[45]

38. On January 26, 2006, the Commission announced the settlement of its case against ChoicePoint, requiring the company to implement a comprehensive

---

[42] Federal Trade Comm'n, Enforcing Privacy Promises: Section 5 of the FTC Act, http://ftc.gov/privacy/privacyinitiatives/promises.html; *see, e.g. In the matter of Genica Corp.*, Federal Trade Comm'n File No. 0823113 (Feb. 5, 2009) (Agreement Containing Consent Order) *available at* http://ftc.gov/os/caselist/0823113/090125genicaagree.pdf; *In the matter of the TJX Companies, Inc.*, Federal Trade Comm'n File No. 0723055 (Mar. 27, 2008); *In the matter of Reed Elsevier Inc. and Seisint, Inc.*, Federal Trade Comm'n File No. 0523094 (Mar. 27, 2008) (Agreement Containing Consent Order) *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf; In the matter of Choicepoint, Inc., Federal Trade Comm'n File No, 0523069 (Jan. 26, 2006) (Stipulated Final Judgment) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

[43] *Id*.

[44] Federal Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), http://www.ftc.gov/opa/2008/03/datasec.shtm.

[45] U.S. Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006, available at: http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

information security program, obtain independent security audits for twenty years, and pay $10 million in civil penalties and $5 million in consumer redress.

*The TJX, Reed Elsevier, and Seisint Consent Orders*

39. On March 27, 2008, the FTC obtained consent orders against The TJX Companies, Inc., Reed Elsevier, Inc., and Seisint, Inc.[46] The orders arose from the companies' failures to provide reasonable security to protect sensitive customer data, and the resulting data breaches.[47]

40. The Commission charged that TJX "created an unnecessary risk to personal information by storing it on, and transmitting it between and within, its various computer networks in clear text."[48]

41. The orders require that the companies implement comprehensive information security programs and hire independent third-party security professionals to review the programs biennially for twenty years.[49]

*The Compgeeks.com Consent Order*

42. On February 5, 2009, the FTC obtained a consent order against Compgeeks.com.[50] The order arose from a FTC complaint that the company "fail[ed] to provide reasonable security to protect sensitive customer data," and the resulting data breaches.[51]

43. The order requires the company to implement "a comprehensive information security program that is reasonably designed to protect the security,

---

[46] Federal Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), http://www.ftc.gov/opa/2008/03/datasec.shtm.
[47] *Id*.
[48] *Id*.
[49] *In the matter of the TJX Companies, Inc.*, Federal Trade Comm'n File No. 0723055 *available at* http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf; *In the matter of Reed Elsevier Inc. and Seisint, Inc.*, Federal Trade Comm'n File No. 0523094 *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.
[50] Federal Trade Comm'n, Consumer Electronics Company Agrees to Settle Data Security Charges; Breach Compromised Data of Hundreds of Consumers (Feb. 5, 2009), http://ftc.gov/opa/2009/02/compgeeks.shtm.
[51] *Id*.

confidentiality, and integrity of personal information collected from or about consumers," and obtain biennial security audits for twenty years.[52]

GOOGLE'S INADEQUATE SECURITY IS AN UNFAIR BUSINESS PRACTICE

44. Google provides Cloud Computing Services to millions of consumers, and encourages consumers to store personal, sensitive information on the services.

45. Prior to the Google Docs Data Breach, Google knew that Cloud Computing Services are susceptible to data breaches.

46. Google knew that disclosure of personal user data could cause substantial injury to consumers, without any countervailing benefits.

47. Google was aware that commonsense security measures, including storing user data in encrypted form, rather than in clear text, could reduce the likelihood and extent of consumer injury.

48. Google knew that a data breach could expose sensitive user data stored on Google Cloud Computing Services. But the company created an unnecessary risk to users' data by employing unreasonable security practices, including the storage and transmission of personal information on its computer network in clear text.

49. As a result of Google's inadequate security practices, the Google Docs Data Breach exposed consumers' personal information to other users of Google's cloud computing service.

GOOGLE'S INADEQUATE SECURITY IS A DECEPTIVE TRADE PRACTICE

50. As described above, Google encourages consumers to save personal data to the company's Cloud Computing Services, and repeatedly assures users that it will safeguard their information.

51. Consumers had every reason to rely on Google's explicit security promises, and such assurances go to the heart of consumers' concerns regarding Cloud Computing Services.

52. Consumers' justified privacy expectations were dashed by the Google Docs Privacy Breach, an incident that exposed users' personal information.

[52] *In the matter of Genica Corp.*, Federal Trade Comm'n File No. 0823113 *available at* http://ftc.gov/os/caselist/0823113/090125genicaagree.pdf.

## CONCLUSION

53. The Google Docs Data Breach highlights the hazards of Google's inadequate security practices, as well as the risks of Cloud Computing Services generally. The recent growth of Cloud Computing Services signals an unprecedented shift of personal information from computers controlled by individuals to networks administered by corporations. Data breaches concerning Cloud Computing Services can result in great harm, which arises from the centralized nature of the services and large volume of information stored "in the cloud." Past data breaches have resulted in serious consumer injury, including identity theft. As a result of the popularity of Cloud Computing Services, data breaches on these services pose a heightened risk of identity theft. The FTC should hold accountable the purveyors of Cloud Computing Services, particularly when service providers make repeated, unequivocal promises to consumers regarding information security.

## REQUEST FOR RELIEF

54. Open an investigation into Google's Cloud Computing Services, specifically concerning:

    a. the adequacy of Google's privacy and security safeguards regarding storage of personal information on its Cloud Computing Services; and

    b. the sufficiency of Google's privacy and security safeguards in light of the company's assurances to consumers regarding its Cloud Computing Services.

55. Require Google to revise its Terms of Service with respect to Cloud Computing Services, including but not limited to Gmail, Google Docs, Google Desktop, Picasa, and Google Calendar, so as to make clear the company's ongoing, affirmative obligations to safeguard the security and privacy of the data that it obtains.

56. Compel Google to make its information security policies more transparent, and to disclose all incidents of data loss or data breach to the Federal Trade Commission.

57. Enjoin Google from offering Cloud Computing Services until safeguards are verifiably established.

58. Compel Google to contribute $5,000,0000 to a public fund that will help support research concerning privacy enhancing technologies, including encryption, effective data anonymization, and mobile location privacy.

EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully submitted,

Marc Rotenberg, esq.
EPIC President

John Verdi, esq
EPIC Counsel

Anirban Sen, esq.
EPIC Fellow

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW Suite 200
Washington, DC 20009
202- 483-1140 (tel)
202-483-1248 (fax)

March 17, 2009