THE UNIVERSITY OF CHICAGO
THE LAW SCHOOL

1111 East 60th Street | Chicago, Illinois 60637
phone 773-702-2087 | fax 773-702-0730
e-mail omri@uchicago.edu
home.uchicago.edu/omri

Omri Ben-Shahar
Leo Herzel Professor in Law
Director, Coase-Sandor Institute for Law and Economics

The Failure of Transparency

Testimony of Professor Omri Ben-Shahar, University of Chicago
Before
Committee on Energy and Commerce
Subcommittee on Communications and Technology
Subcommittee on Digital Commerce and Consumer Protection

Introduction and Summary

The massive collection of people's personal information by companies impacts consumers' privacy and security. At present, the primary and almost exclusive way in which consumers are protected is through "transparency": requiring that companies disclose to consumers what information they collect and how they use it, and alert consumers in the event of a data security breach.

I am a professor of law at the University of Chicago, specializing in consumer markets. I have studied the effects of mandated disclosures in the area of data privacy and in every other area of consumer protection. My research, summarized in a recent book titled "More Than You Wanted To Know" (Princeton, 2014), concludes that disclosure rules are entirely ineffective.

Transparency is intended to strengthen competition in the market. Mandated disclosures are aimed at helping consumers make informed choices and inducing companies to act honestly. It was Louis Brandeis who, 100 years ago, said "sunlight" is "the best of disinfectants." But disclosure rules have miserably failed to achieve their goals. Massive amounts of evidence show that people don't read the disclosures and don't use them to make more informed choices. In reality, disclosures are regularly ignored. They are an empty ritual.

It is tempting to think that disclosures can be more effective if designed to deliver information to consumers in simpler formats. But simplification, too, has been tried for decades and failed. My research shows that simplified disclosures about data privacy and security will have no effect on the behavior of consumers or the companies that collect their information.

Thus, if members of Congress believe that the collection of consumers' data poses risks that require legal intervention, I advise that they look for regulatory solutions that are outside the popular but unsuccessful repertoire of disclosure and transparency.

Disclosure is the Primary Protection Under the Law

The collection of consumers' personal information by companies poses two fundamental challenges. The first is privacy: much of the information collected is personal and sensitive. The second is security: the information may be hacked or stolen and then used in ways detrimental to consumers' financial safety.

American law imposes few practical limits on the collection of personal information by companies. It also does not establish concrete standards for data protection and security. Instead, the most common protection for privacy and data security is "transparency": that any collection or security breach of personal data be accompanied by full and conspicuous disclosures to consumers. Much of the attention of lawmakers, judges, and commentators is directed to "shine the light"—to guarantee that full disclosures are in place to help consumers make more informed and safe choices.

Unfortunately, disclosure regulation has largely failed. And there is little reason to hope that it will ever succeed. Disclosures' failures have a long and persistent history, occurring without exception in every domain of consumer protection. The evidence of failure is abundant, and it is largely uncontested in the literature.

Mandated disclosure is the primary tool of data privacy protection. Our legal environment is packed with statutes and regulations that prohibit various types of data collection or surveillance, but almost all such prohibitions may be waived by consumers. If the consumer agrees, almost any personal information may be collected. It is exceedingly easy for companies to get consumers to agree to waive the statutory protections. It only takes a click "I agree" to the "terms and conditions" or the "privacy notice" (legal texts that regularly contains thousands of words). In fact, a click is not even necessary—the requirement of "informed consent" is satisfied if companies prominently post their privacy notices" on their webpages. Because companies largely comply with the disclosure requirements, the great majority of courts are finding that consumers are effectively agreeing to the data collection, rendering it perfectly legal.

American law also imposes few specific regulations on the security and protection of consumers' information. Businesses are encouraged by the FTC to engage in "best practices" in the storage and safeguarding of consumers' data, but the most concrete obligation is, again, disclosure. For example, under California law businesses are required to "disclose the breach of the security . . . in the most expedient time possible and without unreasonable delay." (California Civil Code, Sec. 1798.82).

The Allure of Disclosure

Transparency is the most common technique of consumer protection not only in the area of privacy and data security. It is the primary tool for protecting borrowers, investors, medical patients, homebuyers, insurance policy holders, internet users—every sector with its array of mandated disclosures. In each of these areas, people are

making choices that are often complex and could severely impact their well being, and are doing so without being fully aware of the risks and benefits. The solution seems alluringly simple: if people make poor decisions because they have poor information, give them more information! Don't people want to make decisions for themselves, and to make them well? Isn't more information better than less? Wouldn't people gratefully take and earnestly use information they are offered?

Because it is so sensible, and because it is thought to be at worst harmless, the mandated disclosure technique is a political winner. Disclosure laws have no enemies as they resonate with almost all American ideologies. Disclosure laws appeal to free-market proponents and to progressives alike, to Democrats and Republicans, even to budget hawks. In almost every area, disclosure mandates and "sunshine laws" are enacted with almost no opposition. Even business interests acquiesce, as they prefer disclosure mandates to more intrusive command-and-control regulations.

Mandated disclosure is alluring because its failures are little noticed and soothingly explained. Lawmakers and commentators do not realize that it is a method so extensively tried, and so they readily attribute any documented failure to the particular way the disclosure was implemented. Maybe the disclosure failed because it was too narrow, or maybe too broad. Maybe it failed because it was too short, or maybe too long. Maybe it was recited to the consumer prematurely, or maybe it was given too late in the game. Maybe it was too technical. Excuses abound.

The Failure of Disclosure

Mandated disclosure is alluring, but it routinely fails to achieve its ambitious goals. Empirical studies show that disclosures rarely change the decisions that people make. People don't read the disclosures. If they read, they do not understand the texts, often written at superior levels of literacy. And even if the texts are written in lay language, they cannot use them profitably because the information conveyed is complex and using complex information to make good decisions requires experience and expertise.

The problem with mandated disclosures is not just their length and complexity. It is also their accumulation. Because disclosures have been enacted in so many areas for so long, people are swamped with disclosures, notices, and warnings of all types. Consumers have become numb to these rituals, viewing them as annoying "fine print" that can be safely ignored. Consumers' apathy is entirely rational: there is simply not enough time to review all the disclosures that the law requires companies to bestow upon them. Just to read all the privacy notices a typical person receives every year would take—according to an estimate done a decade ago—76 days of full time reading, with the loss of productive time costing the economy $781 billion. And, recall, privacy notices are only a small fraction of the sum total of mandated disclosures consumers receive.

Much evidence shows that the disclosure of information is almost irrelevant. Consumers ignore mortgage and banking disclosure (how could they not, given the length and complexity of such documents?) Warnings about product risks or conflicts of interests, medical consent forms, even food and nutrition labels—are all falling upon deaf ears. The evidence is strikingly disappointing: "transparency" requirements have not improved the market outcomes for consumers in any meaningful way.

The Failure of Simplification

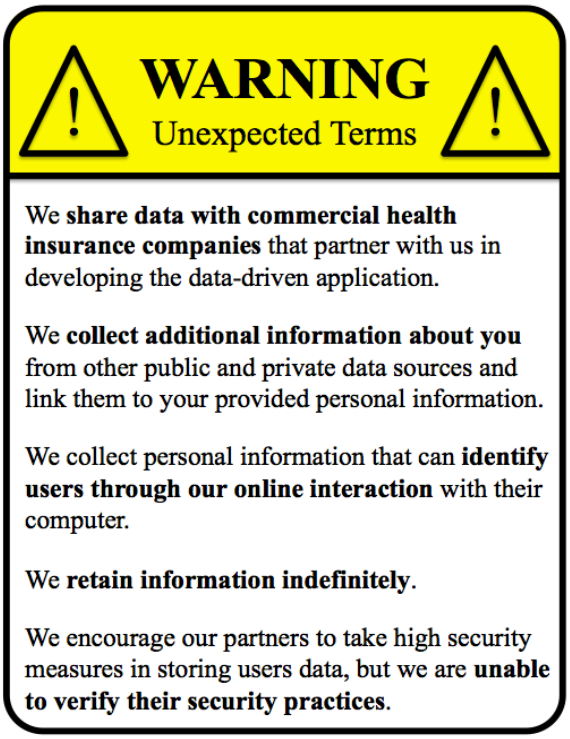
Can disclosure be done more effectively? If existing disclosures are defeated by complexity, can simplicity save them? Could the formats of disclosure be reengineered to become more accessible to consumers and more effective? Simplification seems like an obvious solution. If a disclosure is too long, shorten it. It it's too technical, make it more user-friendly. If it's poorly presented, improve the formatting.

Simplification faces a paradox: if you give people less than full information they may overlook some risks; but if you give them full information they might find the disclosure too long and unmanageable. The pragmatic solution is to focus consumers' attention to the most crucial information and present it in non-technical, easily comparable, format.

Many kinds of simplification strategies along this line have been tried in various areas, with little or no success. Even the simplest of all disclosures—the truth-in-lending's "APR" score that has to be presented before consumers take a loan—has demonstrably failed to improve borrowing decisions. More recent "behaviorally-informed" disclosures, designed by social scientists schooled in diagnosing peoples' decisional failures, have similarly yielded deeply disappointing effects. Such "smart disclosure" designs are required, for example, under federal credit card laws, but have generated only small, almost microscopic, impact on consumers' behavior.

In my own research, I have examined various formats of simplified privacy disclosures. I tested whether people who engage in activity that raises heightened privacy concerns are prompted to act prudently when shown well-designed privacy warnings. I discovered that no matter how simple and conspicuous the warning, consumers' behavior is unchanged. It doesn't matter if the privacy warning is cluttered (as many currently are), or instead drafted according to the FTC's "best practices" guidelines. It doesn't even matter if the privacy notice is pared down to a simple warning box, similar to the familiar Nutrition Facts box (see image below). The simplification of the disclosure has no effect. Consumers don't read the warning one way or another, and imprudently share the same amount of personal information, regardless of the disclosure's format.

Simplification is failing, and this should not be a big surprise. Is it really possible to simplify the complex? Disclosures are long and tiresome because the information necessary to make good decisions about unfamiliar issues is complex and nuanced.



"Warning Label" Privacy Disclosure

Beyond Disclosure

I wrote a book about the failure of disclosure titled "More Than You Wanted to Know." I presented my findings and conclusions—that mandated disclosure fails and cannot be fixed—to numerous audiences. Most agree with my claims, because they know from their own experience that they, too, don't read and are not being helped by disclosures. Still, at the end I am always asked, "What, then? If not disclosure, what does work?"

Unfortunately, there is no one-size-fits-all solution, no new panacea. Different problems merit different solutions. In the area of data privacy and security, it is necessary to begin by identifying the harm from which consumers have to be protected. Collection of information by companies is not harmful in itself. The great majority of consumers are happy to pay for excellent services with their data rather than with money. Some research shows that consumers are not willing to pay more than a few dollars to prevent the harvesting of their data by websites they visit or apps they use. The various class action lawsuits that allege privacy violations have so far failed to robustly demonstrate actual concrete injuries. Moreover, markets seem to be providing some protection: companies that collect sensitive information implement great safeguards. Adult websites, for example, are far more restrictive than other platforms about data sharing; and cloud storage services have higher data security standards. Data security breaches are not harmful unless the data is used for fraudulent transaction. A legal scheme insuring consumers against such losses may be necessary to the extent that consumers are not already protected or insured.