

FTC Settles Computer Spying Charges with Several Companies

SEPTEMBER 27, 2012

A software design firm and seven computer rent-to-own companies have settled charges with the Federal Trade Commission that the companies spied on consumers through software surreptitiously installed on rented computers. The software design firm, DesignerWare LLC, licensed software to several players in the rent-to-own business. The software—known as PC Rental Agent—enabled the rent-to-own store licensees to track and report the physical location of a rented computer and to disable the computer if a consumer is late in making payments. Consumers were not always notified that the company had installed PC Rental Agent on a rented computer. Most importantly, PC Rental Agent included an add-on program called “Detective Mode.” Detective Mode could log keystrokes, take screen shots of users’ computer activities, and use a computer’s web cam to photograph anyone within view of the computer. In addition to these features, Detective Mode offered licensees the option to prompt users with a fake software registration window, prompting a user to enter name, address, e-mail address, and phone number. This information is then transmitted to DesignWare, which in turn gives it to the rent-to-own company that rented out the computer. The FTC worked with the Illinois Attorney General’s office in bringing this case, and alleged several violations of the FTC Act against the software design firm and the rent-to-own companies. These included the “unfair” acts or practices of gathering personal information through the Detective Mode, and using geo-location tracking software without obtaining permission from the computer’s renter. The FTC also alleged that use of the fake registration prompt was “deceptive” under the FTC Act. The proposed settlements ban the companies from using monitoring software like Detective Mode, deceiving consumers into providing information, using geo-location tracking software without notice and consent, and gathering information by using fake registration windows.

TIP: While it might seem reasonable to use technological safeguards to protect computer equipment, companies should be careful not to use tracking technologies without clear notice and consent. This case is a reminder that these issues are on the forefront of the minds of both the FTC and state attorneys general.

2 Min Read

Related Topics

Online Privacy

Consumer Privacy

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.