FTC Sues Uber for Unlawful Subscription Practices

If you run a subscription-based SaaS or tech business and have not reviewed your subscription practices lately, the FTC is again putting you on notice that subscription practices are an oversight and enforcement priority for the federal agency.

The FTC just recently filed suit against Uber Technologies, Inc. and Uber USA, LLC in the Northern District of California on April 21, 2025, alleging that the defendant utilized deceptive billing and cancellation practices. A copy of the FTC complaint is attached at this **link**. A copy of the press release issued by the FTC on the case is **linked here**.

The key factual allegations of the complaint include as follows:

- Consumers were promised a specific amount of savings that did not take into account the monthly price of the subscription.
- Consumers say they were charged without their consent, and in some cases were charged when they did not even have an account.
- Consumers say they were charged before their billing date, including before their free trials ended, despite being promised by Uber that they could cancel at no charge during their free trials.
- Consumers say that it was extremely difficult to cancel, and that they were often charged the renewal subscription fee while they were waiting on customer service to respond and grant the cancellation.

The FTC alleges that Uber's deceptive billing and cancellation practices violate the FTC Act and the Restore Online Shoppers' Confidence Act ("ROSCA"). According to the FTC, these

regulations require online retailers to do the following:

- clearly disclose the terms of the service;
- obtain consumer's consent before charging them for a service; and
- provide a simple method to cancel recurring subscriptions.

In particular, the FTC alleges in its complaint that Uber failed to clearly and conspicuously disclose before obtaining consumer billing information all the material terms of the transaction, including

- that they are being enrolled in a recurring paid subscription;
- the amount of money that consumers in these subscriptions actually save;
- when they will be billed or charged; and
- the method of cancellation.

According to the FTC, Section 4 of ROSCA, 15 U.S.C. § 8403, prohibits charging consumers for goods or services sold in transactions effected on the Internet through a negative option feature, as that term is defined in the Commission's Telemarketing Sales Rule ("TSR"), 16 C.F.R. § 310.2(w), unless the seller provides text that "clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information, obtains the consumer's express informed consent for the charges, and provides simple mechanisms for a consumer to stop recurring charges."

Also, the FTC claims that the TSR defines "negative option feature" to constitute a term in an offer or agreement for goods or services "under which the customer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer."

What are the lessons to be learned from the Uber case by companies operating under a subscription model—particularly SaaS and other technology companies?

First, prior to obtaining credit card information from a consumer, provide clear and very obvious notice of all the material terms of the subscription, including:

- the fact that the consumer is enrolling in a recurring paid subscription;
- the cost of the subscription;
- the frequency of the billing;
- how to cancel.

Second, make sure you have records that this notice was provided to the consumer.

Third, make sure that you have a very simple method for cancellation, i.e. the "click to cancel button," and refrain from engaging in conduct that appears to frustrate cancellation.

Fourth, refrain from making promises or other statements that are not true about promotions or discounts.

These same lessons apply to any subscription or membership; however, SaaS and tech companies providing software to consumers via a subscription model should review their subscription practices today to ensure that they are in compliance with these best practices. If you have questions or concerns about your company's current subscription or membership practices, **schedule a consultation** today with The Prinz Law Office to discuss.

FTC Announces Final “Click to Cancel” Rule for Subscriptions, Memberships

The Federal Trade Commission (“FTC”) has just announced the final version of its “Click to Cancel” Rule for consumer subscriptions. The Rule will go into effect 180 days after it is published with the Federal Register. This Rule will directly apply to all SaaS, digital health, tech, and non-tech companies selling on a subscription basis to consumers.

Full Text of FTC Rule

The full text of the FTC Rule is linked here, at pages 222-230.

Fact Sheet of FTC Rule

The FTC has also made available a fact sheet which briefly summarizes key provisions of the “Click to Cancel Rule,” which is attached here.

Key Provisions of the FTC Rule

According to the FTC announcement, the “Click to Cancel” Rule will apply to “almost all negative option programs in any media.” The key provisions of the FTC Rule will prohibit:

- misrepresenting any material fact made while marketing goods or services with a negative option feature;
- failing to “clearly and conspicuously disclose” material terms prior to obtaining a consumer’s billing information in connection with a negative option feature;
- failing to obtain a consumer’s express informed consent to the negative option feature before charging the consumer; and

- failing to provide a simple mechanism to cancel the negative option feature and immediately stop the charges.

Revisions to Final Version of the FTC Rule

Also according to the FTC announcement, the FTC dropped from its final Rule an annual reminder requirement that would have required vendors to provide annual reminders to consumers advising them of the negative option feature of their subscription, as well as a requirement that vendors had to ask canceling consumers for approval before a vendor could tell a canceling subscriber about reasons to keep the existing agreement or of possible modifications that could be made without canceling the subscription.

Reasons for Adoption of the Rule

Why did the FTC adopt a Click to Cancel Rule? According to the FTC Announcement, the FTC was receiving 70 consumer complaints per day over negative option programs, and this number was "steadily increasing over the past five years."

The FTC's announcement follows a recent California enactment of a more comprehensive "Click to Cancel" law.

Does the FTC Rule Supersede California Law?

The FTC Rule should not supersede California's more comprehensive law; in fact, the Rule specifically states in its text that the Rule will not be construed to supersede any State statute, regulation or order "except to the extent that it is inconsistent with the provisions of this part, and then only to the extent of the inconsistency." The expected impact of the FTC Rule is primarily to bring federal regulatory law closer to California regulatory law as it pertains to subscriptions and memberships.

What do SaaS, Digital Health, Tech, and other Companies Utilizing the Subscription Model Need to do in Response to this Announcement?

All companies utilizing a subscription model should revise consumer contracts and processes to comply with the FTC Rule over the next 180 days. Companies utilizing the subscription model with a business-focused customer base should similarly consider what changes to make to their contracts and processes as public policy will likely change regarding subscriptions generally along with the new FTC Rule and California law changes.

If you have questions or concerns about how new FTC “Click to Cancel” Rule or the new California ”Click to Cancel Law” will impact your digital health company, please schedule a consultation at https://calendly.com/prinzlawoffice.

Kristie Prinz Discusses FTC Suit Over Annual Paid Monthly Software Subscription Plans

Software Lawyer Kristie Prinz discusses FTC concerns with annual paid monthly software subscription plans in this video recorded 7.17.24.

FTC Seeks to Expand Scope of "Negative Option Rule" to Apply to Subscriptions

The FTC has just filed a complaint against a Silicon Valley software company over its "Annual Paid Monthly" subscription contract. The FTC has separately also sought the expansion of its "Negative Option Rule" to amend the provisions to specifically apply to subscriptions by adding a "Click to Cancel" provision. A copy of the FTC notice of proposal is linked here.

What is the FTC's Negative Option Rule?

The Negative Option Rule was adopted by the FTC in 1973, to address "negative option offers," which the FTC defines as offers containing "a term or condition that allows a seller to interpret a customer's silence, or failure to take an affirmative action, as acceptance of an offer."

According to the FTC, negative option marketing utilizes four types of offers: prenotification plans, continuity plans, automatic renewals, and free trial conversion offers.

However, the FTC's original Negative Option Rule only pertained to prenotification plans, excluding the continuity plans, automatic renewals and free trial offers that have become commonplace in 2024. Also, in the case of the original Negative Option Rule, prenotification plans were limited to the sale of goods, where sellers provided periodic notices to participating customers and then sent and charged for those goods only if the consumers took no action to cancel and decline the offer (i.e. the example of a wine club).

Also, the Negative Option Rule required clear and conspicuous disclosure of certain terms before a subscription agreement

was reached. According to the FTC, those terms were as follows:

- how subscribers must notify the seller if they do not wish to purchase the selection;
- any minimum purchase obligations;
- the subscribers' right to cancel;
- whether billing charges include postage and handling;
- that subscribers have at least ten days to reject a selection;
- that if any subscriber is not given ten days to reject a selection, the seller will credit the return of the selection and postage to return the selection, along with shipping and handling; and
- the frequency with which announcements and forms will be sent.'

Finally, under the existing Negative Option Rule, sellers were required to define particular periods for sending merchandise, to give consumers a defined period to respond, to provide instructions for rejecting merchandise, and to promptly honor written cancellation requests.

What is "Click to Cancel'?

What would change with the FTC's newly proposed "Click to Cancel" amendment?

Under the FTC's proposed "Click to Cancel" rule change, the scope of the Negative Option Rule would be increased to make it pertain to not only prenotification plans but also to continuity plans, automatic renewals, and free trial conversion offers. Also, the proposed "Click to Cancel" rule provisions would mandate the following:

- Businesses would be required to make cancelling a subscription or membership at least as easy as it was to start it;
- Businesses would have to ask consumers if they want to

hear new offers when they ask to cancel before they would be able to pitch new offers;
- Businesses would be required to provide an annual reminder if enrolled in a negative option program involving anything other than physical goods, before they are automatically renewed.

Another "Click to Cancel" change is that the under the new provisions any misrepresentation of a material fact related to any of the four negative option offers, whether expressly or by implication, would constitute a violation of not only the Negative Option Rule but also an unfair or deceptive act or practice in violation of Section 5 of the Federal Trade Commission Act.

What is the Potential significance of "Click to Cancel" to the SaaS, Tech, and Digital Health Industries?

The potential significance of the "Click to Cancel" change to the average SaaS, tech, and digital health company is that, if this proposed rule is adopted, SaaS, tech, and digital health companies who sell directly to consumers will need to update consumer contracts and terms of service to confirm that they are compliant with the requirements of the Negative Option Rule, as amended.

If your company is concerned about its compliance with "Click to Cancel" please schedule a consultation today at https://calendly.com/prinzlawoffice.

Is a Company Liable for Software Defects, when a Vulnerability is Discovered but Not Exploited?

If you are in the software business, you likely recognize that you can be sued for materially breaching contracts, infringing third party IP, and data breaches but you may not realize the extent of your liability just for making the sale of a software product deemed to contain a security flaw in the first place, even if the security flaw was never exploited and only identified.

Increasingly, however, just the act of selling software later deemed to be "defective" due to security flaws has resulted in liability to companies.

The Federal Trade Commision (the "FTC") has recently imposed fines and put in place ongoing oversight on companies for this type of issue.

But as Cisco just discovered, if the sales were made to a federal or state agency, the mere act of making the sale can also result in significant liability. Cisco has agreed to pay $8.5 million to settle a case originally filed in New York Western District Court in 2011 involving the sale of video surveillance technology to a variety of government organizations, including but not limited to Homeland Security, the Secret Service, the Army, the Navy, the Marines, the Air Force and the Federal Emergency Management Agency.

According to **The New York Times**, the Cisco case was initiated by the Justice Department in the Federal District Court for the Western District of New York, and the allegations were based on violations of the False Claims Act, which addresses

fraud and misconduct in federal government contracts. Fifteen states and the District of Columbia joined in the suit. As **The New York Times** reported, the argument made by the government was that the software had no value because if failed to serve its primary purpose of security enhancement. According to **The New York Times**, the flaw was identified back in 2008 by a Cisco subcontractor, who brought it to the company's attention at that time. However, as **The New York Times** reported, the subcontractor was subsequently terminated, and when he realized two years later that the vulnerability was still not fixed, he contacted the FBI. **The New York Times** reported that Cisco continued to sell the software with the flaw until July 2013, when if finally notified customers and fixed the flaw.

While the Cisco case applies only to sales made to government, a class action suit is pending right now on similar facts, where the sales were made to non-government consumers. The class action lawsuit was initiated late last year against Symantec for critical defects in its security products under the Norton Brand. It is not clear as to the status of that litigation.

The bottom line: if you are selling software that provides security functionality, you need to have internal systems in place to identify security flaws and quickly fix the flaws, particularly if the software is being sold to a government organization. However, if you are selling to the general public, you may still be liable for sales of the software containing security flaws, whether liability is assessed through the FTC or through class action litigation, regardless of the terms of your contract for those sales.

News Update on FTC's Application of Safeguards Rule to Software Company

News Update 7.17.19

Facebook Agrees to Record $5 Billion Settlement with FTC on Privacy Practices

Multiple media outlets are reporting today that the Federal Trade Commission has agreed to settle its case against Facebook on its privacy practices for $5 Billion.

The Wall Street Journal reports that the vote by FTC commissioners was 3-2 in favor of accepting the agreement and split along party lines with the Republican majority favoring the settlement. According to **The Wall Street Journal**, the matter next goes the the Justice Department's civil division for final review.

According to the **Mercury News**, assuming reports are correct, this will be the largest fine imposed to date by the U.S. government on a tech company. **The Washington Post** reports that the fine is more than 200 times higher than any previous fine.

Interestingly enough, **The Wall Street Journal** is reporting that the fine obtained by the FTC exceeds what the European Union could have obtained under its privacy laws.

The Washington Post predicts that the settlement will impose serious consequences on Facebook that go far beyond just a $5 billion fine. However, **The Washington Post** acknowledges that the dissenting commissioners opposed the settlement because they wanted some assessment of personal liability against CEO Mark Zuckenberg; commissioners reportedly decided to accept a settlement without any such assessment in order to ensure that the matter did not end up in litigation.

While controversial, the FTC's enforcement action in this matter still sets a significant precedent for the software industry with respect to the consequences of not protecting data uploaded to or generated by software. Software companies are on notice: the FTC is closely following your privacy practices and may assess fines in the billions of dollars against you if you fail to take sufficient steps to protect user data.

FTC Sends Warning to IoT Companies on the Importance of Secure Software Development with Enforcement Action Against D-Link

Internet of Things ("IoT") companies are on notice: the FTC is concerned about the the security of software installed to IoT and smart home products and is prepared to take enforcement action against companies to ensure that consumers are protected.

The FTC has just announced the proposed settlement of its case against D-Link filed in January, 2017, which mandates that D-Link put in place and maintain a comprehensive software security program for the next 20 years that incorporates certain specified requirements, including a "secure software development process" that incorporates specified software development safeguards to ensure the security of its devices.

These FTC imposed requirements include the following:

- Specifying in writing how functionality and features secure the devices;
- Engaging in threat modeling to identify potential security risks;
- Reviewing every planned release of code with automated static analysis tools;
- Performing pre-release vulnerability testing on each planned release of code;
- Performing ongoing code maintenance to address vulnerabilities as they are identified;
- Adopting remediation processes to address identified security flaws at any stage of the development process;
- Monitoring research on possible vulnerabilities to devices;
- Setting up a process for receiving and validating vulnerability reports from security researchers;
- Making automatic firmware updates to devices;
- Notifying customers at least 60 days in advance of any decision to stop making security updates to a devices; and
- Providing biennial security training for personnel and any vendors involved with the device software.

In addition to imposing the above requirements on D-LInk, the order gives the FTC the power of oversight to ensure ongoing compliance, and requires D-Link to obtain routine third party assessments by a professional with credentials specified by the FTC to perform in-depth reviews of D-Link's security

practices. The FTC specifically mandates that the assessment meet an approved standard as defined by the FTC: the International Electrotechnical Commission ("IEC") standard for the secure product development life cycle. The FTC announcement is attached **here** and its order is **attached here.**

What prompted the FTC case against D-Link? The FTC complaint filed against D-Link alleged a failure by D-Link to take "reasonable" steps to secure software constituting "unfair acts or practices in or affecting commerce, in violation of Section 5 of the FTC Act, 15 U.S.C. Sections 45(a) and 45 (n)" and misrepresentations regarding D-Link's security practices constituting a "defective act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S. C. Section 45(a)." The FTC Complaint against D-Link is attached **here**.

What do companies engaged in IoT software development need to take away from this enforcement action? First of all, companies need to be aware that the FTC is applying its regulatory powers against companies to ensure that they are securing software in accordance with any representations made to consumers. Second of all, companies need to be aware that the FTC is looking to certain published standards by the IEC to provide the industry standards for software in this space, so IEC compliance certification may provide the measure of a company's compliance with its security obligations. Third, the FTC has provided some suggested guidelines for companies to follow in the following publications: **Careful Connections: Building Security in the Internet of Things** and **Start With Security: Lessons Learned from FTC Cases.**

FTC Puts Software Companies and Service Providers on Notice of Broad Enforcement Powers Under Gramm-Leach-Bliley Act Safeguards Rule

The Federal Trade Commission ("FTC") has put software companies and software service providers on notice it intends to interpret the Gramm-Leach-Bliley Act's Safeguards Rule broadly to apply to businesses which make available software or services that serve financial, payroll, and accounting purposes and collect sensitive data on consumers and their employees.

The FTC recently announced its settlement of a complaint filed against LightYear Dealer Technologies, LLC which does business as Dealerbuilt, which required Dealerbuilt as condition of the settlement to develop, implement and maintain an information security program that incorporates the minimum requirements specified by the FTC and submit to third party compliance assessments and annual certifications over a period of the next 20 years.

The FTC's specified minimum requirements for Dealerbuilt's information security program included the following:

- Develop, implement, maintain and record in writing an Information Security Program;
- Make available the written program, evaluations of the program, and updates on the program, to the company's board of directors or governing body, or if none exists, the senior officer responsible for the program at least once per annual period and after any data breach;

- Identify an employee or employees responsible for the coordination of the program;
- Provide written assessment annually and after any data breach of any potential data breach risks;
- Develop written safeguards to ensure data security including the following:
    - Training of all employees at least once every annual period on how to protect personal information;
    - Technical measures monitoring networks, systems to identify attempted data breaches;
    - Access controls on databases containing personal information, which (a) restrict the ability to connect to only approved IP addresses; (b) require authentication to access the databases; and (c) limit the access of employees to only those databases as necessary to perform their duties;
    - Encrypt all social security numbers and financial account information;
    - Implement policies and procedures for secure installation and inventory on an annual basis
- Perform assessment annually and after any data breach of the sufficiency of safeguards and modify the program as necessary;
- Conduct test annually and after any data breach of effectiveness of safeguards, which shall include vulnerability testing every four months and after a data breach, and annual penetration testing, as well as after any data breach;
- Ensuring that contracts with any service providers ensure compliance with safeguards; and
- Evaluate and make adjustments to program upon any changes to operations or business or in event of any data breach. or on an annual basis.

The FTC Order also mandates that an information security assessment be conducted initially and biennially by a third

party professional approved by the Associate Director for Enforcement for the Bureau of Consumer Protection at the FTC, and that the assessor will be required to provide the documents relevant to the assessment to the FTC for review within 10 days following the completion of the initial review and then on demand. Furthermore, the Order requires the senior corporate manager or senior officer of Dealerbuilt to submit annual written certifications to the FTC, and that within a reasonable time following any discovery of a data breach, or at least 10 days following the provision of first notice of any data breach, Dealerbuilt must send a report to the FTC of any data breach, which meets certain specified requirements. Also, the Order permanently enjoins all individuals affiliated with Dealerbuilt from violating any provisions of the Safeguards Rule, and makes the Order applicable to all businesses connected to Dealerbuilt, which Dealerbuilt is to be broadly interpreted and Dealerbuilt is required to identify in detail via compliance reports, accompanied by sworn affidavits.

The FTC also imposes broad recordkeeping requirements on Dealerbuilt through the Order, requiring Dealerbuilt to create and retain for the next 20 years accounting records of all revenues collected, personnel records, consumer complaint records and responses to those records, and any documents relied upon to prepare mandate assessments and to demonstrate full compliance with the order.

Finally, within 10 days of any request by the FTC, Dealerbuilt is required to furnish compliance reports to the FTC or other requested information accompanied by sworn affidavits.

The FTC announcement is attached **here** and the Order attached **here**.

What prompted this broad enforcement action by the FTC against DealerBuilt? According to the **FTC Complaint**, a series of security failures resulted in the breach of a backup database

through a storage device beginning in late October 2016, which resulted in the breach of personal information of nearly Seventy Thousand consumers, which included full names and addresses, telephone numbers, social security numbers, drivers license numbers, and birthdates of consumers as well as wage and financial account information of dealership employees. The **FTC Complaint** further alleges that Dealerbuilt failed to detect the breach and only learned of it after a customer called its chief technology officer demanding to know why customer data was publicly available on the Internet.

The **FTC Complaint** alleged that Dealerbuilt was a financial institution as defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6809(3)(A) as a result of being "significantly engaged in data processing for its customers, auto dealerships that extend credit to customers." **The Complaint** alleged that the "failure to employ measures to protect personal information" constituted an "unfair act or practice" and that the failures to (a) "develop, implement, and maintain a written information security program"; (b) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information" and "assess the sufficiency of any safeguards in place to control those risks"; and (c) to design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards" constituted a violation of the Safeguards Rule and an unfair or deceptive act or practice in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

What should software companies and service providers take away from this FTC enforcement action? First and foremost, the FTC is making a definitive statement that if you are in the business of providing software or software services that have any sort of financial or accounting function to them, you are a financial institution for purposes of Gramm-Leach-Bliley and the Safeguards Rule is going to be deemed to apply to your

business. Second, the FTC considers service providers accountable for the protection of any personal data they collect or store. Third, the FTC expects businesses using third party software or providers to have contracts in place with those software companies or service providers imposing security requirements, monitoring requirements, and explicitly requiring them to follow websites reporting on known vulnerabilities. Fourth, the FTC expects businesses to train and supervise employees on how to ensure the security of the company. The FTC specifically points businesses in its announcement to comply with its publication, **Start with Security: Lessons Learned from FTC Cases**.FTC Puts Software Companies and Service Providers on Notice of Broad Enforcement Powers Under Gramm-Leach-Bliley Act Safeguards Rule

---

Recent FTC Enforcement Actions Should Serve as a Warning to Software Industry Regarding Privacy Practices

If your company is like most and you have given little or no thought to your company's privacy policy while also collecting data and looking for ways to monetize it, then you may want to rethink how you are operating in light of recent enforcement actions by the FTC in the user data space. The Silicon Valley Software Law Blog addressed these developments in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/recent-ftc-enforcement-actions-should-serve-as-warning-to-software-industry-about-

privacy-practices/

FTC Announces Order Against San Francisco Software Company

The FTC has issued an order against a San Francisco software company for deceptive and misleading trade practices with respect to the distribution of the software product and with respect to advertising and promotions related to the software product. The Silicon Valley Software Law Blog has provided a brief summary of the complaint and the order issued by the FTC in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/ftc-announces-approval-of-final-order-in-deceptive-app-case-against-vulcan

---

FTC Signals to Health Software Companies an

Intention to Increase Scrutiny over Advertising Claims

The FTC has just reached a settlement with Lumos Labs over claims that the company was deceptively advertising the health benefits of its Luminosity software program. The FTC's action over this issue should serve as a warning to the health software industry regarding how health software companies are advertising their products. The Silicon Valley Software Law Blog further addressed this matter in the following blog post:
http://www.siliconvalleysoftwarelaw.com/lumos-labs-case-signals-to-health-software-industry-an-intention-by-the-ftc-to-police-advertising-claims

---

Google Settles with FTC over In-App Purchases Made by Children

The Federal Trade Commission has announced that Google has agreed to refund customers' unauthorized in-app purchases made by their children in the Google Play Store, as the Silicon Valley Software Law Blog discussed in its recent blog posting attached below:

http://www.siliconvalleysoftwarelaw.com/ftc-settlement-with-google-to-require-refund-of-unauthorized-in-app-charges

$163 Million Damage Award in Federal Case Against Scareware Software Company and Founders

The U.S. District Court for the District of Maryland has awarded damages in excess of $163 million in a FTC case against a “scareware” software company, Innovative Marketing, Inc. and its founders, as further discussed by the Silicon Valley Software Law Blog in the blog post link below:

http://www.siliconvalleysoftwarelaw.com/federal-court-awards-163-million-judgment-against-scareware-software-company-in-ftc-case

---

FTC Proposing New Rules to Protect Children’s Online Privacy

FTC has announced that it is proposing an amendment to the Children’s Online Privacy Protection Rule (“COPPA”). The Silicon Valley Software Law Blog discussed the proposed changes as well as the pros and cons of potential implementation in its blog posting linked below:

http://www.siliconvalleysoftwarelaw.com/ftc-proposing-new-rules-to-protect-childrens-online-privacy

---

FTC’s Suit Against Intel: What Will Be the Impact on the Silicon Valley?

The Silicon Valley IP Licensing Law Blog discussed the likely impact of the FTC’s lawsuit against Intel on Silicon Valley in the following blog post:

http://www.siliconvalleyiplicensinglaw.com/ftcs-suit-against-intel-what-will-be-the-impact-on-the-silicon-valley/.

IP Law 360 Reporter Sara Stefanini Interviews Silicon Valley Life Sciences Lawyer Kristie Prinz for “In Cephalon Case, FTC Hopes for

High Court Ruling”

Click here to read the article