Privacy & Security Law

Perkins Coie’s Privacy & Security group represents some of the world’s leading internet companies, wired and wireless communications providers, brick-and-mortar retailers and emerging online businesses.

Data and security breaches are increasingly headline news and the current legal climate includes complex and nuanced rules governing the collection, use, storage, and disposal of information that vary by jurisdiction and is continually evolving. We work closely with our clients to help them stay abreast of national and international regulatory and statutory changes and industry initiatives related to mobile applications, online and mobile advertising, means of capturing location information, and cloud computing. We are ranked by Chambers USA among the best firms in the nation for privacy and data security. We also were recognized by Law360 as a “Practice Group of the Year” in 2013.

Areas of Focus:

PRODUCT AND GENERAL PRIVACY AND SECURITY COUNSELING

We routinely review products and services to identify and resolve privacy and data security issues. These reviews cover privacy policies, disclosures and terms, and also include an in-depth understanding of the data flows involved in the company’s products or services. Representative projects include:

- Helping clients launch social components to large retail e-commerce sites
- Advising on product privacy on mobile applications
- Guiding on roll-outs of new web-based payment processing services
- Drafting policies for data sharing with cloud service providers
- Designing compliance programs to launch international services in more than 60 jurisdictions

We have extensive experience helping clients develop data security policies and programs needed to comply with PCI Data Security Standards, Red Flag Rules, HIPAA, GLBA, COPPA, TCPA, FERPA, FCRA, CAN-SPAM, FTC guidelines, state data protection laws, as well as self-regulatory rules.

ELECTRONIC SURVEILLANCE AND USER INFORMATION REQUESTS

We provide training and advice to clients in complying with surveillance laws and responding to requests for customer information. We also regularly advise clients and litigate on their behalf on issues related to their obligations under the:

- Wiretap Act
- Pen/Trap Statute
- Stored Communications Act
- Foreign Intelligence Surveillance Act
- National Security Letters
- Communications Assistance for Law Enforcement Act

ONLINE AND MOBILE ADVERTISING

As advertising models increasingly rely on user data, regulatory scrutiny of the collection and use of information of all types from browsers and mobile apps continues to increase. Representative experience includes:

- Helping companies draft meaningful and accurate disclosures of their advertising practices, including how to provide “just in time” notice
- Counseling on how, and under what circumstances, clients should offer choice with respect to data collection and use practices, and what form such choice should take
- Training on compliance with self-regulatory rules and state and federal consumer protection statutes, the Children’s Online Privacy Protection Act (COPPA), and state laws governing advertising to minors
- Counseling major technology companies, web publishers and online retailers on responding to web browser-based “do not track” signals

We counsel advertising technology companies, communications providers, and web and mobile application publishers on how to structure their practices in a manner that is consistent with self-regulatory rules as well as regulatory and legal frameworks. We have deep experience with self-regulatory bodies, including the Network Advertising Initiative, Digital Advertising Alliance and Better Business Bureau, regarding online behavioral advertising and mobile advertising issues.

**PRIVACY REVIEWS, ASSESSMENTS AND DATA TRANSFERS**

Privacy assessments are rapidly becoming an important part of every business that handles customer or user information. Before a company can fully appreciate its obligations and risks, or implement “privacy by design,” it needs to “know its data,” which means that it needs to understand what types of user information it collects and uses, where the data is stored, with whom the data is shared, and when and how the data is disposed.

To help companies fully understand their collection, use and sharing of personal and other sensitive data, we conduct comprehensive privacy reviews. Retailers, telecommunication providers, power companies, cloud providers and international companies are among the companies for whom we have provided reviews. Contexts in which we have performed privacy assessments include:

- Launch of new and existing products
- Mergers and acquisitions
- Cloud, advertising and other transactions where the transfer of personal information across international boundaries is an issue

Honed during repeated engagements, our approach to gathering data is efficient as we assist in or conduct onsite interviews. Our custom reports offer specific and practical recommendations and checklists to help our clients quickly understand the data they handle and the myriad laws and regulations that apply to their collection, use, storage and sharing of that data.

After conducting an assessment, we work closely with clients to prioritize needed remedial efforts. Privacy assessments make this follow-on work seamless and efficient. The assessment process provides us with a unique level of detail to thoroughly understand our clients’ data collection and use practices. Examples of follow-up projects include:

- Counseling related to individual products that were evaluated during the review
- Drafting incident response or disaster recovery plans
- Creating corporate information management programs
- Helping companies certify in the EU Safe Harbor program in order to lawfully transfer to the United States data about their European customers or employees

**NETWORK INTRUSIONS AND DATA BREACHES**

Our data breach and network intrusion response team includes several former DOJ cybercrime prosecutors. We regularly counsel clients with concerns about data breaches and assist with coordinating incident response and required notifications. We have helped clients, ranging from public Fortune 100 companies and retailers with operations and customers nationwide to local nonprofits, school districts and small private companies, work through legal requirements and address their legal, reputational and commercial risks.

Lost, stolen or inadvertently disclosed electronic or physical records containing the personal information of users, customers or employees - not to mention trade secrets and intellectual property - implicate a web of state and federal laws and regulatory interest.

While not every breach involves a type of personal information that requires notification or disclosure, every breach requires attention and an individualized response tailored to the facts and nature of the breach, and an evaluation of how processes can be improved to minimize the risk of future breaches. Features of our service include:

- An efficient approach that includes triaging the initial breach, minimizing legal risk, identifying notification and disclosure obligations, and providing notice to affected individuals, regulators and others where necessary
- Capabilities to tap into existing relationships with forensics firms and breach notification providers when the size or nature of the breach warrants
Addressing publicly traded companies’ need for disclosures in security filings pursuant to the SEC’s guidance on disclosing cybersecurity risks

Advice and counsel on network intrusions, such as companies’ obligations as the victim of an attack, and the steps necessary to remediate compromised networks

Perkins Coie’s counsel includes extensive experience in helping clients avoid breaches through targeted product advice, privacy assessments and other counseling centered on understanding a company’s data and instituting programs to prevent and detect intrusions.

**PRIVACY LITIGATION AND REGULATORY INVESTIGATIONS**

Our attorneys help clients respond to regulatory inquiries from the FTC, FCC and state attorneys general. We assist in favorably resolving regulatory inquiries through our quick understanding of the client’s technology and by providing the agencies with the appropriate information to understand our client’s practices. Examples of our counsel to technology companies in regulatory investigations include:

- Represented Google in negotiation of first FTC “privacy by design” and EU Safe Harbor consent decree regarding Google Buzz
- Defended Google before regulatory bodies worldwide, including the FTC and a multistate attorneys general investigation, in inquiries stemming from Google’s Wi-Fi data collection via Street View
- Represented a Fortune 50 company in connection with multiple criminal and civil inquiries by government agencies regarding alleged collection and sharing of subscriber data without consent
- Protected numerous mobile applications and mobile advertising companies in defense of FTC inquiries presenting issues under Section 5 of the FTC Act and also COPPA

Often, regulatory investigations lead to, or are simultaneous with, private-party class action litigation involving claims based on privacy policy statements, consumer protection laws prohibiting deceptive or unfair practices, collection and disclosure of user information, TCPA, ECPA and SCA, and California Song-Beverly Act claims. We have specific experience coordinating the defense of both regulatory and class action litigation stemming from the same occurrence, which requires careful navigation of different timelines and different discovery requirements.

We also routinely collaborate with attorneys in our Class Action Defense group, which has significant experience in managing and successfully defending consumer protection class action litigation. Examples of privacy-related class actions include:

- Represented Google in multiple nationwide class actions regarding privacy issues, including those regarding Google Buzz and regarding Google Play/Google Wallet
- Defended Twitter in class action regarding privacy issues related to uploading of mobile device address books
- Represented Sprint in putative class actions asserting claims under federal and state privacy laws

**CYBER ENFORCEMENT**

Our cyber enforcement group helps clients protect their websites, Internet and mobile services, and keep users safe from abuse. We have dedicated Internet investigation resources that help us identify, understand and document sophisticated schemes that target our clients and are instigated by spammers, hackers, phishers, scrapers, scammers and other computer system abusers and criminals.

We advise clients on effective enforcement strategies that may include referrals to regulatory agencies, referrals to law enforcement, or filing civil lawsuits against the wrongdoers. Perkins Coie also efficiently implements enforcement programs and readily adapts services to meet client needs. These programs may range from a single cease and desist letter and follow-up, to multifaceted, multiyear programs where a company outsources its enforcement work to our dedicated team of Internet enforcement lawyers.

**INTERNATIONAL PRIVACY AND DATA FLOWS**

Our clients operate around the world, which requires global guidance that allows them to move data in compliance with international privacy laws. Worldwide privacy challenges include data transfers, cross-border evidence gathering, investigations, civil discovery, employment matters, processing agreements, and mergers and acquisitions. Perkins Coie provides international privacy counsel in areas such as:

- Compliance with non-U.S. law enforcement data requests and Mutual Legal Assistance Treaty requests
- eDiscovery outside the U.S., and response to civil demands, Section 1782 requests and other civil matters
- Defense of multijurisdictional privacy inquiries
We work with local counsel around the world to meet domestic privacy requirements, and we assist companies to conduct global data assessments and respond to data breaches.

TCPA COMPLIANCE AND DEFENSE

Any company that places calls or sends text messages to customers does so against the backdrop of an extremely aggressive plaintiffs’ class action bar eager to bring claims under the Telephone Consumer Protection Act (TCPA). Perkins Coie counsels companies on avoiding TCPA lawsuits and defending them when facing TCPA claims, and we represent companies before the FCC in rulemaking and enforcement proceedings.

With a team bolstered by former FCC, in-house, and industry advertising group attorneys, and a national class action defense practice, we counsel clients regarding all aspects of TCPA compliance. This includes compliance with recent TCPA amendments regarding prior express written consent and novel technologies, such as group texting, refer-a-friend features, lead generation and the interplay between TCPA and HIPAA, among other issues. We also regularly represent a wide variety of organizations in TCPA lawsuits and regulatory proceedings.

Representative matters in which we have provided TCPA counsel include:

- Defended Google in a TCPA class action relating to a group messaging platform
- Represented Limited Brands in a TCPA class action in the Northern District of Illinois
- Represented NASCAR in defense of a TCPA class action claim relating to text messages
- Represented Quicken Loans in successfully moving to dismiss three of four causes of action and obtaining discovery sanctions on a TCPA cause of action resulting in dismissal of remaining TCPA claim
- Obtained a dismissal with prejudice for Redbox in a TCPA class action in California federal court
- Defended Career Education Corporation in two separate class actions alleging violations of the TCPA for the sending of text messages promoting educational institutions
- Represented Sprint and achieved a settlement on a class-wide basis, obtained preliminary approval and final approval of the settlement, and worked with a claim administrator to receive and settle claims
- Represented a communications provider in an FCC investigation regarding TCPA issues and negotiated a settlement with the FCC’s Enforcement Bureau
- Filed petitions for declaratory rulings with the FCC on behalf of Outspoken and TextMe
- Represented Obama for America in a TCPA class action alleging that robocalls were made to cell phones without consent

To keep clients current on litigation and regulatory developments, we produce a newsletter on emerging issues on TCPA and related privacy issues.

We regularly advise clients on how to implement "privacy by design" principles into their organizations, and how to best respond to law enforcement and civil requests for user information, sophisticated network attacks and other security breaches. Our data breach and network intrusion response team, including several former DOJ cybercrime prosecutors, regularly counsels clients with concerns about data breaches and assists with coordinating incident response and required notifications.

"Privacy by design," privacy assessments, security breach response plans, insurance coverage and contractual provisions for transferring data and securing it, are all tools for developing a successful privacy program. Privacy plans also must address responding to consumer complaints, litigation or regulatory inquiries. We help our clients respond to immediate issues and understand that it is never too late to address privacy and security matters.

EXPERIENCE

WORTH UNLIMITED, LLC V. REDDIT, INC.
Superior Court of California, San Francisco County
Successfully defended motion to compel production of the identity of an anonymous speaker pursuant to domesticated subpoena in connection with out-of-state litigation.

WILLIAMS V. T-MOBILE USA INC.
Circuit Court of Michigan, Wayne County
Defended T-Mobile against pretexting related claims.

VIRTUAL PROPERTY AND REAL MONEY TRANSACTIONS
Assisted virtual property trading platform company with regulatory compliance related to electronic payment systems and real money transactions.

**VALENTINE, ET AL. V. NEBUAD INC., ET AL.**  
U.S. District Court for the Northern District of California
Represented Internet service providers WOW and Knology in a putative class action in which Internet subscribers alleged violations of federal and state privacy laws arising from the defendants' use on a trial basis of the NebuAd system. The system was designed to allow ISPs to serve targeted advertisements to their customers browsing the Web. Each of the ISP defendants was an out-of-state provider with no customers in California. Case dismissed on the grounds that the court lacked personal jurisdiction.

**USER WEBSERVICE**  
Federal Trade Commission
Represented webservice in Federal Trade Commission investigation under Section 5 of the FTC Act regarding user data privacy. Investigation closed.

**SUPNICK V. ALEXA INTERNET AND AMAZON.COM INC.**  
U.S. District Court for the Western District of Washington
Defense of purported nationwide class action challenging privacy practices related to information collected during visits to Web sites.

**SECURITY BREACH RESPONSE**  
Provide counsel to numerous clients on the legal requirements following a data breach incidents, including the need for and content of consumer and regulator notifications, investigation and public relations. Advise on creation and modification of incident response plans. Supervise the maintenance of the security breach notification laws chart, which surveys the state laws that require notification in the event of security breaches involving the loss of personal data.

**PRIVACY COUNSELING**  
Provide counsel to clients on a variety of issues surrounding the collection and use of personal data, including compliance with the Fair Credit Reporting Act (FCRA), Red Flag Rules, the Children's Online Privacy Protection Act (COPPA), CAN-SPAM, Family Educational Rights and Privacy Act (FERPA), Federal Trade Commission guidance and statute statutory and common law requirements. Draft privacy policies conforming to companies' data practices and applicable legal requirements.

**MOBILE ADVERTISING NETWORK**  
Federal Trade Commission
Represented mobile advertising network in defense of Federal Trade Commission investigation under Section 5 of the FTC Act. The Commission sought information about specific categories of advertisements displayed to consumers on mobile applications and the network’s screening practices. Investigation closed.

**MILLER V. SMART & FINAL INC.**  
Lead counsel for retailer in putative nationwide class action alleging violation of the Fair Credit Reporting Act (FCRA).

**MANARD V. KNOLOGY, INC.**  
U.S. District Court for the Middle District of Georgia
Represented Internet service provider Knology in a putative class action in which Internet subscribers alleged violations of federal and state privacy laws arising from the ISP's use on a trial basis of the NebuAd system. The system was designed to allow ISPs to serve targeted advertisements to their customers browsing the Web. Successfully obtained order compelling arbitration of claims. No. 4:10-CV-15, 2010 WL 2528320 (M.D. Ga. June 18, 2010).

**MAESTRINI V. SMART & FINAL INC.**  
Lead counsel in putative California Consumer Class Action alleging violation of State's Point of Sale privacy laws. Case dismissed with prejudice prior to certification.

**INTERNET ENFORCEMENT—FORTUNE 500 RETAILER**  
Led campaign against online scams that used infringing domain names, misleading websites, and false text messages to lure consumers into buying goods and services and disclosing personal information. Significantly reduced scams and consumer complaints regarding scams.

**INTERNET ENFORCEMENT—FACEBOOK**  
Ongoing management of a complete enforcement program for Facebook Inc. to enforce its Terms of Use; prosecute spammers, hackers and phishers; and to investigate and refer illegal behavior to law enforcement.

**INTERMARINE, LLC V. SPLIETHOFF BEVRACHTINGSKANTOOR**  
U.S. District Court for the Northern District of California
Successfully moved to quash federal deposition subpoena issued to Dropbox, obtaining published order holding that providers like Dropbox do not need to make themselves available for testimony every time a subscriber's records are at issue in a case.
INQUIRY INTO GOOGLE WIFI DATA COLLECTION VIA STREET VIEW
Represented Google before regulatory bodies globally, and in litigation, regarding Google’s WiFi data collection via Street View. Successfully obtained closing letter from the Federal Trade Commission, completing its investigation.

IN THE MATTER OF GOOGLE INC.
Federal Trade Commission
Successfully represented Google before the Federal Trade Commission in defense of FTC complaint regarding launch of Google Buzz social networking application and Gmail user privacy. The resulting consent decree was the first FTC privacy and EU Safe Harbor settlement. Assisted the company in implementation of the privacy program described in the consent decree.

IN RE GOOGLE BUZZ PRIVACY LITIGATION
U.S. District Court for the Northern District of California
Represented Google in defense of consolidated nationwide class actions challenging Google Buzz social networking application for alleged violations of Gmail user privacy. Settlement approved by the court.

IN RE FACEBOOK, INC.
U.S. District Court for the Northern District of California
Successfully moved to quash subpoena, issued pursuant to 28 U.S.C. § 1782 seeking the content of social media communications belonging to a deceased user.

HOANG V. AMAZON.COM, INC. AND IMDB.COM, INC.
U.S. District Court for the Western District of Washington
Successfully represented Amazon.com, Inc. and IMDb.com, Inc. in defense of breach of contract, fraud, Consumer Protection Act, and Washington Privacy Act claims relating to IMDb.com’s online publication of the plaintiff’s accurate date of birth. Obtained successful summary judgment disposition for Amazon.com, and a unanimous defense verdict for IMDb.com following a jury trial.

FACEBOOK ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) COMPLIANCE PROGRAM
Counseling and litigation related to subpoenas, court orders, warrants and other requests for user information subject to the ECPA, Stored Communications Act and other federal and state statutes.

ELECTRONIC SURVEILLANCE AND USER DATA DISCLOSURE COUNSELING
Assist communications service providers in developing procedures to comply with lawfully authorized electronic surveillance orders and user data disclosure requests, both domestically and internationally, primarily in accordance with the Electronic Communications Privacy Act (ECPA).

CROWLEY V. CYBERSPACE CORPORATION
U.S. District Court for the Northern District of California
Successful defense of putative class action challenging privacy practices of retailer and credit verification service. 166 F. Supp. 2d 1263 (N.D. Cal. 2001)

CRAIGSLIST.COM WEBSITE ENFORCEMENT PROGRAM
Pre-litigation investigation, enforcement program and litigation related to Internet infringement of craigslist’s copyrights, trademarks and terms of use violations.

COUNSELING: MONEY TRANSMISSION AND ANTI-MONEY LAUNDERING
Provide comprehensive counseling regarding compliance with state and federal money transmission laws as they relate to emerging payment systems, and in particular decentralized virtual currency business ventures. Develop and implement anti-money laundering programs, conduct related risk assessments, and represent clients before state and federal regulators like FinCEN and state departments of financial services.

CLOUD COMPUTING PROVIDER
Federal Trade Commission
Represented cloud computing provider in Federal Trade Commission investigation under Section 5 of the FTC Act regarding security practices for mobile access to cloud computing service. Investigation closed.

CHANCE, ET AL. V. AVENUE A INC.
U.S. District Court for the Western District of Washington
Defense of nationwide class action challenging Internet privacy practices. Settled after successful summary judgment motion. 165 F. Supp. 2d 1153 (W.D. Wash. 2001)

ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM DEALING WITH EMERGING PAYMENT METHODS
Worked with national car association to develop anti-money laundering compliance program addressing traditional payment services, such as money transmission and consumer credit, as well as new payment products and services, such as open loop gift cards and P2P services.

NEWS
11.01.2019

**Partner Dominique Shelton Leipzig Quoted in Axios - The Global Shortage of Privacy Experts**

General News

Axios

Dominique Shelton Leipzig was quoted in the Axios article, "The Global Shortage of Privacy Experts," on the importance of hiring a privacy expert for every company—not just big technology companies.

10.24.2019

**Dominique Shelton Leipzig Quoted in Law.com - Few State Breach Laws Include Biometrics, But That Could Soon Change**

General News

Law.com

Dominique Shelton Leipzig was quoted in the Law.com article, "Few State Breach Laws Include Biometrics, But That Could Soon Change," regarding the increasing awareness of privacy and security among individuals.

PUBLICATIONS

Revised September 2019

**Security Breach Notification Chart**

Attorney Publications

Perkins Coie's Privacy & Security practice maintains a comprehensive chart of state laws regarding security breach notification. The chart helps keep clients informed about each state's sometimes-unique security breach notification requirements. Lawyers, compliance professionals, and business owners have told us that the chart has been helpful when preparing for and responding to data breaches.

11.01.2019

**Avoiding CCPA-Related Insurance Gaps**

Articles

Risk Management

Beginning January 1, 2020, companies doing business in California that meet certain criteria will be subject to a new regulation, as the sweeping California Consumer Privacy Act (CCPA) goes into effect.

10.30.2019

**The Proposed CCPA Regulations Impose New Obligations**

Updates

The California Attorney General's Office released for public comment the long-awaited proposed regulations for the California Consumer Privacy Act (CCPA) on October 10, 2019.

10.2019

**California: CCPA Proposed Regulations and More**

Articles

OneTrust DataGuidance

On 10 October 2019, after much anticipation, the California Attorney General, Xavier Becerra, held a press conference and announced the release of proposed regulations, intended to further the purposes of the California Consumer Privacy Act of 2018 (CCPA).

10.16.2019

**New California Ballot Initiative Contemplates Stricter Privacy Requirements**

Updates

A new California privacy ballot initiative has been introduced by real estate developer and privacy rights advocate, Alastair Mactaggart.

09.23.2019

**Privacy Issues in Business Combinations**

Articles

Global Banking & Finance Review

Every buyer of a U.S. business needs to think about what liabilities it is acquiring in the transaction and how to minimize or eliminate those liabilities or to become comfortable with the liabilities.

09.20.2019

**CCPA Amendments Provide Important Clarification**

Updates

While privacy laws are proliferating globally, the California Consumer Privacy Act (the CCPA) is California's comprehensive and landmark legislation that seeks to give California consumers expanded rights to learn about and control certain aspects of how a business handles “personal information” collected about its consumers.
China’s New Draft Encryption Law

Updates

The Standing Committee of the National People’s Congress released the Encryption Law of the People’s Republic of China (Draft) for public comment on July 5, 2019 (the ‘2019 Draft’).

PRESENTATIONS

10.29.2019

The Evolution of Security & How to Adapt to Ensure Your Organization Is Secure Online
Speaking Engagements
Moderator/Panelist
Illinois Technology Association / Chicago, IL

10.10.2019

Complying with New York’s SHIELD Act
Speaking Engagements
TechGC CLE Webinar / New York

09.25.2019

Speaking Engagements
Moderator, CCPA Panel

09.23.2019

Understanding the CCPA
Speaking Engagements

09.23.2019

What the U.S. Regulatory Landscape Means for Your Privacy Program
Speaking Engagements

CONTACTS

Todd M. Hinnen
Partner
Seattle
D +1.206.359.3384

Thomas (Tom) C. Bell
Partner
Seattle
D +1.206.359.8845

RELATED SERVICES

PRACTICES
• Ad Tech Privacy & Data Management
• Biometric Law
• Business Litigation
• Corporate Law
• Intellectual Property Law
• Litigation
New California Ballot Initiative Contemplates Stricter Privacy Requirements

A new California privacy ballot initiative has been introduced by real estate developer and privacy rights advocate, Alastair Mactaggart.

Security Breach Notification Chart

Perkins Coie's Privacy & Security practice maintains a comprehensive chart of state laws regarding security breach notification. The chart helps keep clients informed about each state's sometimes-unique security...

States Continue to Expand Breach Notification Requirements in 2019

As more and larger data breaches come to light, states continue to update and expand their breach notification statutes, adding to the patchwork of notification obligations that now exists...
Introduction and Comments on Measures for Data Security Management in China
The Cyberspace Administration of China (i.e., the Office of the Central Cyberspace Affairs of China) promulgated the draft *Measures for Data Security Management* (the Measures) for...

New York and New Jersey Make an Early Effort to Regulate Artificial Intelligence
In recent years, the use of artificial intelligence (AI) solutions in every sphere of the economy has increased dramatically. In response to its rapid growth, governments are scrambling to...

FCC Continues Uphill Battle Against Unwanted Robocalls

Regulating the Security of Connected Devices: Are You Ready?
As if businesses did not have enough on their plates as they prepare for the California Consumer Protection Act and similar privacy laws in other states, manufacturers of Internet of Things (IoT) devices (objects...
Nevada Grants Consumers Opt-Out Rights in Expanded Online Privacy Law
Nevada is the latest state to strengthen privacy laws to address the perceived need for more oversight of how companies handle personal data.

European Parliament Approves Amendments to Draft “Terrorist Content” Legislation
The European Parliament approved several amendments to the European Commission’s proposed Regulation on preventing the dissemination of terrorist...

PRIVACY QUICK TIPS BLOG
Your Practical Guide to Privacy, Data Security and Data Management
The blog provides practical tips and updates on emerging privacy and data security issues, with a focus on operational incorporation of privacy/data security principles in a business environment.

GENERAL DATA PROTECTION REGULATION (GDPR)
Perkins Coie’s Privacy & Data Security lawyers have a deep understanding of the GDPR requirements for both data controllers and data processors, and regularly counsel companies doing business in the EU to help them meet the GDPR’s requirements.