

## DATA PRIVACY & SECURITY

### OVERVIEW

BCLP's Global Data Privacy and Security team is composed of lawyers located across the United States, the United Kingdom and continental Europe, and Asia. We routinely advise clients in a variety of sectors, including hospitality, consumer services, healthcare, software and technology, financial services, travel, manufacturing, and retail. We coordinate advice across multiple jurisdictions for clients working to achieve the most streamlined international data privacy strategy as possible, and we excel at helping companies achieve their business goals while balancing and addressing privacy and security obligations in a practical, business-focused approach. We pride ourselves on our responsiveness and building teams shaped to meet our clients' needs.

### AI LEGISLATION & REGULATION TRACKERS

US state-by-state

AI legislation snapshot

To help companies achieve their business goals while minimizing regulatory risk, our team actively tracks proposed and enacted AI regulatory bills from across the United States to enable our clients to stay informed in this rapidly-changing regulatory landscape.

UK and EU

UK and EU take divergent approaches to AI regulation

As companies increasingly integrate AI into their products, services, processes, and decision-making, they will need to do so in ways that comply with the varying regulatory approaches in the UK and EU. Our UK and EU AI Regulation Tracker will keep you updated on legislation t...

### Privacy Advisory

Our team has extensive experience handling the full scope of complex privacy and security issues. From a data privacy perspective, we advise clients on the development of comprehensive privacy and data protection programs, data sharing and international mobilization of data, complex transactions involving monetization and licensing of data, as well as with conducting gap

assessments to align with international privacy standards, responding to regulatory investigations and inquiries, and defending companies in court and before government agencies in enforcement actions.

This counseling spans the gamut of US and non-US privacy laws, including the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, state privacy and data breach laws, FTC and state law enforcement issues, as well as emerging laws and regulations around the world.

## **Incident Response and Preparedness**

In the context of incident response and preparedness, we have a world class incident response practice that has helped clients navigate major security incidents and data breaches, including ransomware attacks, O365 mailbox intrusions, malware, credential harvesting, insider threats, and inadvertent disclosure. We leverage that experience to help companies identify and remediate gaps in their readiness and to train companies how to respond to breaches effectively. Should an incident occur, BCLP's 24-hour hotline<sup>[1]</sup> connects clients directly with experienced attorneys who will guide companies through all aspects of breach response, from investigation and notification to regulatory investigation or litigation. Our experience and practical approach to data breach response uniquely equip us to assist organizations by understanding both the law and the business implications of data breaches. We help clients get ahead of incident response issues by providing a range of offerings, including bespoke "drill" exercises with c-suite executives, analysis of insurance coverage, contractual analysis to identify business partners and customers who require notification of a breach, and evaluation and engagement of third party providers under privilege (forensics, PR, call centers).

We are continually working to understand new privacy and security issues and to partner with our clients to shape practical, risk-based solutions that can be adapted over time to ever-changing technologies, business priorities and laws.

## MEET THE TEAM



### **Amy de La Lama**

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial and Government Affairs, Boulder

[amy.delalama@bclplaw.com](mailto:amy.delalama@bclplaw.com)

+1 303 417 8535



### **Geraldine Scali**

Partner, London

[geraldine.scali@bclplaw.com](mailto:geraldine.scali@bclplaw.com)

+44 (0) 20 3400 4483



### **Christian M. Auty**

Partner and US Lead – Data Privacy  
and Security , Chicago  
[christian.auty@bclplaw.com](mailto:christian.auty@bclplaw.com)  
[+1 312 602 5144](tel:+13126025144)



## **Kate Brimsted**

Partner and UK Lead – Data Privacy  
and Security , London

[kate.brimsted@bclplaw.com](mailto:kate.brimsted@bclplaw.com)  
[+44 \(0\) 20 3400 3207](tel:+442034003207)

## **AREAS OF FOCUS**

- BCLP Data Breach Hotline
- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act

## **EXPERIENCE**

- Defending a major online fashion retailer in a lawsuit alleging violation of the Video Privacy Protection Act. The suit alleges that the client hosts video content on its website and that by also using Facebook pixels on its website to track usage statistics, it is unlawfully sharing personally identifiable information concerning videos viewed by users with a third party, in violation of the VPPA.
- Defending a provider of crypto currency trading software in a class action lawsuit filed in the wake of disclosures that the company was the victim of criminal hacking. The hacking resulted in the unauthorized disclosure of API keys, which were allegedly used by the hackers to consummate unauthorized trades in user accounts on various crypto currency exchanges.

## REPRESENTATIVE CLIENTS

- Red Robin – Casual dining restaurant chain operating in the U.S.
- Delaware North – Manages and provides food and beverage concessions, dining, entertainment and lodging at high-profile locations throughout the world
- Best Western International – One of the top five largest hotel chains in the world.
- World Wide Technology, Inc. – One of the 100 largest privately held companies in the United States; provides technology needs to national and multi-national companies with revenues in excess of \$7.4 billion annually
- Grindr LLC – Grindr is the premiere platform for the global LGBTQ+ community to connect, learn and champion their rights. With more than 3.8 million daily active users in more than 190 countries, Grindr empowers people to be themselves in a safe and meaningful way. Given the sensitive nature of information disclosed in-app, the company is focused on global compliance with data privacy and security laws.
- Washington University in St. Louis. – Washington University is routinely ranked as one of the top 15 universities within the United States, and one of the top 5 medical schools in the United States.
- IHS Markit Ltd. – Global diversified provider of critical information, analytics, and solutions
- Dillard's Inc. – An upscale department store chain in the U.S. with more than 325 stores in 28 states
- eClinicalWorks – One of the main providers of electronic medical records to physicians and health groups
- Backstop Solutions – Provider of portfolio management technology to financial advisors and hedge funds

## RELATED INSIGHTS

Insights

Apr 08, 2024

**New York May Lead the Pack Through Imposition of Data Excise Taxes**

Insights

Mar 13, 2024

## **GBA Standard Contract to Promote Cross-Border Data Flow**

Insights

Mar 08, 2024

### **What is FemTech and how can it meet the privacy needs of its users?**

In part one of our series "FemTech: how this growing industry can build trust, protect privacy and redress healthcare inequity... one app at a time", we take an introductory look at the industry, and offer some commercially-minded approaches to address users' privacy needs.

Insights

Mar 05, 2024

### **Washington My Health Data Act FAQ's: processing biometric data**

Insights

Feb 16, 2024

### **New TCPA opt-out rules coming as FCC adopts report and order on revocation of consent**

On February 15, 2024, the Federal Communications Commission ("FCC") adopted the Draft Report and Order and Further Notice of Proposed Rulemaking ("Report and Order")[1] that it released last month under the Telephone Consumer Protection Act ("TCPA"). The Report and Order, along with the new Rules, will have major impacts for senders of marketing text messages. Under the TCPA, businesses cannot text marketing messages, make marketing robocalls, or send fax advertisements to a consumer without having obtained their "prior express written consent." [2] The new ruling imposes strict requirements for revocation of consent. Businesses should take note and ensure their opt-out procedures comply with the new rules. Failure to do so may result in a class action lawsuit, as the TCPA provides for a private right of action with statutory damages of \$500-1,500 per violation, per consumer, with n...

Insights

Feb 14, 2024

### **CNIL's Strategic Focus Areas for Data Protection in 2024**

Insights

Feb 12, 2024

### **Colorado adopts universal opt-out requirements**

Webinars

Feb 08, 2024

### **Public Company Update, Cybersecurity Issues and Other Trending Topics**

Insights

Feb 06, 2024

### **Fourth Circuit holds faxes received online not subject to TCPA**

A fax is a fax is a fax or is it? In a recent ruling in the long-running TCPA junk fax case Career Counseling, Inc. v. AmeriFactors Financial Group, the Fourth Circuit Court of Appeals held that the statute's prohibition against uninvited fax advertisements does not apply to faxes received through online fax services. In a very positive development for TCPA defendants, the Court affirmed the denial of class certification for a proposed class including both members who used a traditional fax machine and those who used an online fax service. The Court

reasoned that identifying the traditional fax machine users would require individualized inquiries, which rendered the proposed class unascertainable. While consistent with the Federal Communication Commission’s declaratory ruling from *In the Matter of AmeriFactors Financial Grp., LLC Petition for Expedited Declaratory Ruling* (“FCC Ruling”),<sup>[1]</sup> the decision marks a d...