

Cryptome

15 March 2010

Source:

http://www.cov.com/practice/global_privacy_and_data_security/

DATA SECURITY BREACH EXPERTISE

Our Global Privacy and Data Security Practices has been recognized by *Chambers USA*, among others, as a leading practice. We have assisted clients in responding to scores of security breach situations, including breaches involving millions of records containing personal information. We also have successfully defended numerous clients in regulatory investigations into their privacy and security practices, and have broad litigation experience on cases involving privacy, security, and consumer law issues. And, we have represented several clients in pursuing insurance recoveries for claims and losses arising out of security breaches.

Examples of our work include:

- Representing Microsoft in the FTC's groundbreaking investigation and agreement related to Microsoft's Passport Internet authentication service, which was the FTC's first consent agreement under Section 5 of the FTC Act to impose information security commitments related to the protection of personal information.
- Serving as lead regulatory counsel on both federal and state law for a financial service company in connection with a security breach involving the unauthorized disclosure of millions of bank account and credit card numbers. The matter was resolved with the FTC without any enforcement action.
- Counseling several financial institutions on compliance with Gramm-Leach-Bliley and state law requirements in connection with lost data tapes and other security incidents involving customer account information.
- Counseling a major online company in responding to a security incident affecting the credit card information of more than 200,000 customers, including regulatory inquiries. The matter was resolved without any regulatory enforcement action.
- Successfully defending a client in FTC and New York State AG investigations into the security of information exposed by a hack into FTP servers.
- Representing a multi-national pharmaceutical company in responding to a security incident involving the loss of personal information belonging to more than 100,000 employees, and defending against a subsequent investigation by Connecticut state authorities. The matter was resolved without any formal enforcement action.
- Representing The TJX Companies, Inc. ("TJX") in pursuing insurance recoveries for claims and losses arising out of unauthorized intrusions into TJX's computer systems and the potential theft of confidential information from customers of T.J. Maxx and other TJX retail stores. The claims for which we are pursuing insurance recovery include class action lawsuits brought by both consumers and financial institutions. Our representation, which began shortly after the data breach was publicly announced in January 2007, has involved the analysis and pursuit of multiple lines of insurance coverage, including cyber-risk, general liability, first-party property, D&O, and crime policies.
- Representing Heartland Payment Systems, Inc. with respect to E&O and D&O insurance coverage for numerous class actions arising out of a widely-reported intrusion into Heartland's computer systems.

- Representing Wells Fargo Bank in several putative consumer class actions brought under California's Unfair Competition Law (Section 17200) challenging the bank's disclosures and other practices.
-

If you have any questions concerning the material discussed, please contact the following members of our Global Privacy & Data Security practice:

Erin Egan	202.662.5145	eeagan@cov.com
David Fagan	202.662.5291	dfagan@cov.com
Mark Plotkin	202.662.5656	mplotkin@cov.com
Jamillia Ferris	202.662.5058	jferris@cov.com

GLOBAL PRIVACY & DATA SECURITY

Ranked by a leading IT trade publication as having one of the ten best privacy practices in the world, Covington combines exceptional substantive expertise with an unrivaled understanding of the IT industry, and of e-commerce business models in particular. One of our core strengths is the ability to advise clients on relevant privacy and data security rules worldwide, and to help them structure globally valid compliance programs. In recent years, our global privacy and data security lawyers in the United States and European Union (EU) have helped write landmark legislation, counseled clients on complex transactions, developed compliance strategies covering a wide variety of statutes and regulations, helped respond to numerous security breaches, authored or co-authored multiple treatises, and represented clients in investigations, enforcement actions, and litigation.

Erin M. Egan
eegan@cov.com
202.662.5145

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

Daniel P. Cooper
dcooper@cov.com
44.(0)20.7067.2020

Many of our global privacy and data security lawyers have extensive experience in complementary areas, which enables us to counsel clients thoughtfully and efficiently on the full checkerboard of privacy and security laws. Our attorneys have expertise not only in the IT industry, but also in the telecommunications, media, financial services, health care, labor and employment, and food and drug sectors. Our global privacy and data security attorneys include litigators, transactional lawyers, and legislative and regulatory strategists with decades of high-level experience on Capitol Hill and with federal agencies.

REPRESENTATIVE MATTERS

- We have actively participated in legislative and regulatory efforts involving a range of privacy and data security issues, such as commercial e-mail, phishing, spyware, identity theft, caller ID spoofing, and individual background checks. For example, we worked closely with Hill staff on federal spam legislation and prepared witnesses to testify before the House and Senate Commerce Committees, and we filed comments on the Federal Trade Commission's implementing regulations cited repeatedly by the Commission after the legislation became law.
- We assisted a leading Internet travel company in responding to a data security incident involving the stolen personal information of hundreds of thousands of customers, including preparing notices to consumers and regulators, establishing fraud monitoring and tailored customer service, and working with federal and state officials to ensure compliance with applicable requirements and best practices (and to avoid lawsuits or enforcement actions).
- We advised a leading online company on risk management and affirmative strategies, including potential litigation options, in connection with the unauthorized use and disclosure of customer personal information by a third-party service provider. Based on our advice, the client was able to resolve the potentially difficult situation quickly and on favorable terms.
- We prepared comprehensive legal and ethical guidelines for the use of background checks, collection of personal information, and electronic monitoring for internal investigations by a major information technology client.
- We have helped numerous companies to develop global comprehensive privacy policies, facilitate international data transfers, and structured outsourcing arrangements in compliance with federal, state, EU, and other laws and best practices, including the US-EU Safe Harbor privacy framework.

ACCOLADES

- Covington Privacy & Data Security partners, Erin Egan, Marty Hansen and Mark Plotkin ranked by

Chambers Global as leading lawyers (2010).

- Ranked by *Chambers UK* as a leading Data Protection Practice (2010).
- Covington Privacy and Data Security partners Daniel Cooper and Daniel Pavin ranked by *Chambers UK* (2010).
- Ranked by *Legal 500 EMEA* as a leading EU Regulatory, Privacy and Data Protection practice (2009).
- Ranked By *Chambers USA* as a leading Privacy & Data Security Practice (2009).
- Covington Privacy & Data Security partners, Erin Egan, David Fagan, Martin Hansen, and Mark Plotkin ranked by *Chambers USA* as leading lawyers (2009).
- Ranked by *ComputerWorld* as one of the leading Privacy Consultancies (2008).
- Covington Privacy & Data Security partner, Erin Egan, ranked by *Practical Law Company (PLC)* as a leading lawyer (2006-2007).

COUNSELING & COMPLIANCE

Covington regularly counsels clients in the United States and Europe regarding compliance with laws, regulations, and best practices involving the privacy and security of personal information. We not only evaluate our clients' existing practices, but also offer creative, forward-thinking strategies to maximize new business opportunities within applicable privacy and security standards.

Our counseling and compliance work ranges from assisting clients in conducting privacy and security audits—to assess the ways in which they collect, handle, and protect their customers' personal information—to advising on potential liability arising out of business practices, human resources procedures, marketing plans, and online activities. For example, we work with clients to formulate information security policies that comply with legal standards and best practices, and we often analyze our clients' websites and information practices and proposals for compliance with their stated policies. We offer operational advice on how clients can structure marketing practices to meet federal and state requirements regarding commercial e-mail, telemarketing, direct mail, and advertising. We also advise on appropriate mechanisms to transfer data from the European Union (EU) to the US and assist clients in drafting certification documents under the US-EU Safe Harbor agreement.

Erin M. Egan
eeagan@cov.com
202.662.5145

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

Mark E. Plotkin
mplotkin@cov.com
202.662.5656

REPRESENTATIVE MATTERS

- Work with a wide variety of clients to draft, refine, and implement website privacy policies and provide related advice regarding the operation of those sites, including advice regarding material changes to privacy policies.
- Served as outside counsel to working group of affiliates and subsidiaries of major Internet client that met regularly to discuss privacy issues and methods for streamlining or modifying the client's privacy and security practices.
- Conducted risk assessments of proposals by major pharmaceutical and retail clients to share consumer information with third parties for marketing purposes, and advised clients on options for mitigating risk without compromising business goals.
- Advised pharmaceutical companies in the United States and Europe on data privacy issues relating to genetic testing programs and the development of genomics databases, pharmacovigilance reporting, further use of data collected in clinical trials, the sourcing and handling of human tissue, and biological samples for research purposes, patient outreach, and marketing activities.
- Worked with a multidisciplinary and multi-industry group of privacy representatives that met regularly to explore issues surrounding the development of federal privacy legislation.
- Provided advice regarding a statewide campaign to oppose a March 2004 California ballot initiative imposing customer information-sharing restrictions on financial institutions.
- For a leading aerospace company, conducted an in-depth legal analysis of the application of privacy and data security laws in the United States, Europe, and Asia to new communications technology with employee- and consumer-facing components.

DATA SECURITY

Covington represents clients on a range of matters involving the security of confidential customer, employee, business proprietary, and partner information. Our lawyers have been integrally involved in developing information security policies and conducting assessments of data security practices to comply with legal requirements, regulatory obligations, best practices, and specific agreements with third parties and governmental agencies. We are expert in the legal regimes governing data security both in the United States and the European Union (EU).

We frequently advise clients on all aspects of responding to data security breaches, including conducting investigations, taking appropriate remedial action to protect the integrity of potentially compromised information, working with law enforcement when necessary and appropriate, and notifying consumers and regulators. Our expertise also includes conducting data security audits on behalf of our clients, assessing their existing data security practices and refining their information security policies and incident response plans.

Additionally, we have been closely involved in congressional consideration of data security issues, including drafting testimony on security-related issues for clients and providing comments on various federal proposals governing data security and breach notification requirements. In Europe, we regularly counsel clients on the security standards arising under national and regional data privacy laws, including the detailed security regimes in Italy, Poland, and Spain, and we track developments associated with the European Network and Information Security Agency (ENISA) and European security standardization bodies.

REPRESENTATIVE MATTERS

- Represented clients before Federal Trade Commission and state attorneys general investigations into data security practices. For example, we represented Microsoft in a Federal Trade Commission investigation of statements concerning the data security provided by Microsoft's Passport identity authentication service, including negotiating and supervising compliance with an FTC consent order.
- Counseled numerous clients regarding notification and other remedial measures following breaches of security that potentially compromised personal information. For instance, we helped a leading Internet business respond to a data security incident involving more than 200,000 customers, including preparing notices to customers and regulators and establishing remedial measures in compliance with state laws and best practices.
- Performed data security due diligence for multiple clients in connection with major corporate mergers and acquisitions.
- Advised a Canadian province on the ability of US law enforcement agencies to access business records under the USA PATRIOT Act.
- Prepared compliance guidelines for data security under the Gramm-Leach-Bliley Act and the Health Information Portability and Accountability Act of 1996 for a major provider of outsourced support services — including human resources work, customer service, and recordkeeping — to companies in the financial, health care, and other sectors.

Erin M. Egan

eegan@cov.com
202.662.5145

Henriette Tielemans

htielemans@cov.com
32.2.549.5252

Daniel P. Cooper

dcooper@cov.com
44.(0)20.7067.2020

FINANCIAL PRIVACY

From helping draft key legislation to counseling clients in complying with implementing requirements, Covington's financial privacy lawyers have been at the center of the development of comprehensive and workable rules to protect the privacy of personal financial information. By providing testimony, advice, and representation, we are leading the way on this vital issue affecting our global economy.

Our financial privacy lawyers were extensively involved in the legislative processes that produced Title V of the Gramm-Leach-Bliley Act (GLB Act) and the Fair and Accurate Credit Transactions Act, two important laws regulating the privacy practices of financial institutions. After the laws were enacted, we worked with the banking and financial regulatory agencies, including the Federal Trade Commission, to formulate appropriate regulations implementing the laws.

We regularly advise clients regarding compliance with these and other financial privacy laws and regulations, including issues involving opt-out notice provisions, restrictions on the re-use and re-disclosure of consumer information, security guidelines, and federal preemption of state and local privacy restrictions. We have also advised financial institutions in the European Union (EU) on privacy issues under US and EU law, including compliance with audit and reporting rules under the Sarbanes-Oxley Act, as well as EU privacy and anti-money laundering rules.

Mark E. Plotkin

mplotkin@cov.com
202.662.5656

Henriette Tielemans

htielemans@cov.com
32.2.549.5252

Daniel P. Cooper

dcooper@cov.com
44.(0)20.7067.2020

REPRESENTATIVE MATTERS

- Testified before the Senate Banking Committee and state legislatures on the scope and meaning of the GLB Act's privacy provisions, including repeated and extensive appearances before California legislative committees on pending legislation to increase financial institution privacy obligations.
- Testified before the House Ways and Means Subcommittee on proposals to limit the use of social security numbers as unique identifiers.
- Successfully litigated a leading case advocating Fair Credit Reporting Act preemption of the affiliate-sharing provisions of California financial privacy law.
- Provided advice regarding a statewide campaign to oppose a March 2004 California ballot initiative imposing customer information-sharing restrictions on financial institutions.
- Advised online retailers regarding compliance with the Payment Card Industry standards for the storage, processing, and transmission of credit cardholder data.
- Made presentations to state attorneys general regarding enforcement efforts targeting alleged financial privacy violations.

HEALTH INFORMATION PRIVACY

Covington's health information privacy lawyers have played a key role in the debate over the privacy of medical records and other individually identifiable health information. We serve a broad client base of healthcare providers, pharmaceutical companies, benefit managers, group health plans, clinical laboratories, medical equipment manufacturers, and others whose businesses involve the handling of personal health information. We routinely counsel these clients regarding compliance with the privacy standards promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and we have assisted in our clients' efforts to obtain amendments to, or clarifications of, these regulations. We also counsel our clients on state laws affecting the privacy of certain types of medical records, including genetic information and pharmacy records.

We often assist clients in the United States and Europe engaging in clinical trials and post-marketing research activities, and have been involved in preparing informed consent forms, investigator disclosure documents, Contract Research Organization (CRO) agreements, clinical trial agreements and service provider agreements. Lawyers in our London and Brussels offices have acquired unparalleled expertise in the unique privacy issues facing the pharmaceutical industry in Europe.

Anna D. Kraus

akraus@cov.com
202.662.5320

Henriette Tielemans

htielemans@cov.com
32.2.549.5252

Daniel P. Cooper

dcooper@cov.com
44.(0)20.7067.2020

REPRESENTATIVE MATTERS

- Advised pharmaceutical companies in the United States and Europe on data privacy issues, including questions relating to genetic testing programs and the development of genomics databases, the sourcing and handling of human tissue and biological samples for research purposes, patient outreach, and marketing activities.
- Represented Wyeth in a consumer class action alleging that it violated various privacy rights granted by the California Constitution, the California Confidentiality of Medical Information Act, and common law through its participation in direct mailing programs run by various pharmacies.
- Assisted pharmaceutical companies in developing global comprehensive privacy policies aligned with federal (HIPAA, Food & Drug Administration, and National Institutes of Health), state and European law, and best practices.
- Conducted due diligence regarding a target company's privacy and data security practices on behalf of a client seeking to acquire a healthcare information products company.
- Represent an ad hoc consortium of US and European pharmaceutical and medical device companies concerned about data privacy issues in Europe, including the Eastern European Member States such as Hungary, Poland, and the Czech Republic.
- Advised a large pharmaceutical company in connection with litigation involving the alleged infringement of patient privacy by a pharmacy chain that collects personal information about prescription drug users.

HUMAN RESOURCES PRIVACY

Covington lawyers have helped numerous clients understand and comply with the increasingly complex set of rules governing privacy in the workplace. On a range of issues including the privacy of employment records, employee monitoring, the use of biometrics, and pretexting, our lawyers provide thoughtful and valuable advice to help our clients manage human resources and other workplace operations. Two of our attorneys co-author an annual chapter on employment privacy law in the District of Columbia for a leading treatise.

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

Daniel P. Cooper
dcooper@cov.com
44.(0)20.7067.2020

We regularly advise clients regarding proper methods for collecting and processing employee personal information, including preparing notices, consent forms, and contracts in connection with employment relationships. In addition, we draft acceptable use policies for Internet, e-mail, blogging, and other network activities in accordance with existing laws and practices regarding workplace monitoring. We often undertake detailed reviews of companies' privacy practices in connection with internal audits, as well as proposed transactions, and we offer training and compliance programs to help clients ensure that they are managing employee information responsibly.

Of particular importance to many multinational corporations is the transfer of employee data from Europe or Asia to the United States, and we have helped clients identify the proper legal basis for effecting such transfers. Finally, our lawyers are expert in counseling companies that have suffered security breaches involving employee personal information, and we work with them to develop appropriate responses to affected individuals and regulators.

REPRESENTATIVE MATTERS

- Provided guidance to a major technology and manufacturing company in connection with the unauthorized posting of employee personal information on a third-party webpage. Our efforts on behalf of the client included working with Internet service providers to remove the posted information and providing notice to potentially affected individuals and applicable state regulators.
- Conducted a detailed review of the human resources operations of a large pharmaceutical company to assess compliance with data protection and privacy laws and regulations in both the US and EU, in anticipation of possible certification under the US-EU Safe Harbor regime. Our extensive written report described potential compliance issues and recommended specific remedial actions.
- Advised a major pharmaceutical client on the collection and use of its employees' biometric information and social security numbers for internal purposes.
- Advised a major sports league on the procedures for conducting pre-hire background checks under the FCRA and state law, and drafted appropriate contract language and consent forms accordingly.
- Advised a multinational company on the privacy issues implicated by development of an internal network that could automatically scan the content of employee e-mail during transmission.
- Conducted a pan-European and selective US survey of laws and regulations affecting an employer's right to monitor employee's Internet use and review electronic communications. We have also advised numerous clients on the law governing call recording and access to (and disclosure of) employee e-mail, including in connection with several personal crises and actions.
- Advised numerous clients regarding the privacy implications of conducting an informal internal audit of certain foreign business practices at the request of the U.S. Securities and Exchange Commission.
- Drafted privacy-related provisions for use in data processing and outsourcing arrangements and advised on state and tort-based employee privacy laws in connection with a proposed acquisition.

INTERNET & TELECOMMUNICATIONS PRIVACY

As counsel for many of the world's leading software, Internet, and communications companies, Covington advises clients on a wide range of online privacy issues, including acceptable practices for collection, use, disclosure, access, and security with respect to personally identifiable information. Our attorneys help clients implement and maintain manageable and transparent website privacy policies, and we audit websites for compliance with stated policies. In addition, we counsel companies in the United States and Europe on how to structure their marketing practices to meet federal, state, and European Union (EU) requirements governing commercial e-mail and telemarketing.

We often represent clients before federal and state agencies, working to negotiate agreements and consent orders involving privacy practices. We also frequently consult with legislators and regulators, both in the United States and the EU, in connection with proposed laws and rules involving commercial e-mail, telemarketing, fax advertising, and identity theft.

Erin M. Egan

eegan@cov.com
202.662.5145

Henriette Tielemans

htielemans@cov.com
32.2.549.5252

Daniel P. Cooper

dcooper@cov.com
44.(0)20.7067.2020

REPRESENTATIVE MATTERS

- Developed legal and practical strategies to combat proposed state legislation requiring online dating service providers to conduct background checks of potential customers.
- Successfully challenged before the D.C. Circuit the Federal Communication Commission's rules mandating that telecommunications companies install equipment to monitor private telephone and Internet communications.
- Prepared an assessment for a leading national association on the installation and use of event data recorders ("black boxes") in passenger cars under state law and proposed NHTSA regulations.
- Advised a telecommunications client on strategy, including options for enforcing existing law or drafting legislation, for combating the spoofing of its customers' telephone numbers to subvert caller identification technology.
- Actively participated in legislative and regulatory efforts involving a range of privacy and data security issues, such as commercial e-mail, phishing, spyware, identity theft, caller ID spoofing, and individual background checks. For example, we worked closely with Hill staff on federal spam legislation and prepared witnesses to testify before the House and Senate Commerce Committees, and we filed comments on the Federal Trade Commission's implementing regulations cited repeatedly by the Commission after the legislation became law.
- Negotiated a favorable agreement with the Children's Advisory Research Unit of the Better Business Bureau regarding an Internet service provider's compliance with the Children's Online Privacy Protection Act.
- Advised clients who provide e-mail services to customers and employees on requirements and best practices with respect to the transmission, storage, monitoring, and retention of electronic communications.

- Prepared extensive privacy training materials and participated in training sessions for employees of European subsidiaries of a US-based company.

INVESTIGATIONS & ENFORCEMENT

Covington lawyers have successfully represented clients in numerous investigations involving their privacy and data security practices. Drawing upon our extensive experience before the Federal Trade Commission (FTC) and other agencies, we are able to guide clients confidently and as painlessly as possible through this process, and to achieve favorable outcomes in state and federal enforcement actions.

We have particular expertise in actions brought by the FTC and the privacy authorities of the European Union (EU) and its Member States, often working with regulators to negotiate agreements and consent orders. In addition, we represent clients with respect to claims brought by state attorneys general under consumer protection and unfair practices statutes, including laws relating to public statements regarding online privacy and security.

Charles E. Buffon
cbuffon@cov.com
202.662.5542

Erin M. Egan
eegan@cov.com
202.662.5145

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

REPRESENTATIVE MATTERS

- Successfully defended a client in an investigation by the FTC and the New York State Attorney General into the security of information exposed by a hack into its servers.
- Represented Microsoft in negotiating an FTC Consent Order related to the privacy and security practices involving the company's Passport, PocketPC, and WebTV products and services.
- Advised numerous clients regarding the privacy implications of conducting an informal internal audit of certain foreign business practices at the request of the US Securities and Exchange Commission.
- Advised on the legitimacy of a transfer of European data to the United States pursuant to a US subpoena, and steps to be taken in Europe under EU and national laws.
- Negotiated a favorable agreement with the Children's Advisory Research Unit of the Better Business Bureau regarding an Internet service provider's compliance with the Children's Online Privacy Protection Act.

LEGISLATIVE & REGULATORY ADVOCACY

Many of the firm's efforts in the fields of global privacy and data security involve working directly with legislators and regulators to address emerging public policy issues. We have lobbied, monitored, and advised at both the federal and state levels, and on European Union (EU) and Member State legislation regarding data protection.

Through our practice, we have developed extensive contacts at regulatory agencies, in Congress, and throughout the EU with whom we have worked closely to help shape and respond to the major privacy and security policy issues of our day. We also regularly appear before agencies and legislatures to testify about the implications of various privacy initiatives on both online and off-line activities.

Covington lawyers have been deeply involved in the legislative and regulatory processes that produced key laws in the areas of financial privacy, health information privacy, and children's online privacy. In addition, we were asked to advise the European Commission in connection with implementation of the EU-US Safe Harbor arrangement for the transfer of data to the United States. We also provided expert testimony before EU authorities regarding compliance issues encountered by multinational companies.

Erin M. Egan
eegan@cov.com
202.662.5145

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

REPRESENTATIVE MATTERS

- Testified before the Senate Banking Committee and state legislatures on the scope and meaning of the Gramm-Leach-Bliley Act's privacy provisions, including repeated and extensive appearances before California legislative committees on pending legislation to increase financial institution privacy obligations.
- Testified before the House Ways and Means Subcommittee on proposals to limit the use of social security numbers as unique identifiers.
- Worked with the House and Senate Commerce and Judiciary Committees to develop federal spyware legislation, including preparing witness testimony before the Senate Commerce Committee. Our efforts also included meeting with officials in the Department of Commerce and preparing panelists to speak at FTC workshops regarding spyware.
- Participated in legislative efforts to formulate federal data security legislation, including working with the House and Senate Commerce, Judiciary and Financial Services Committees, drafting amendments and testimony, and attending industry meetings.
- Reviewed and commented on federal spam legislation and prepared witness testimony before the House and Senate Commerce Committees. We also filed comments regarding the Federal Trade Commission's implementing regulations after the legislation was passed into law.
- Consulted with various Eastern European agencies regarding the implementation of national data privacy legislation and compliance with EU requirements.

PRIVACY LITIGATION

Covington's global privacy and data security lawyers include many seasoned litigators who have represented numerous clients in lawsuits involving a broad spectrum of related issues. When our clients face lawsuits alleging privacy or security violations, we respond quickly and efficiently to minimize liability and optimize the chances of success. Likewise, when our clients' rights are violated by others, we develop creative and forward-thinking strategies to vindicate those rights in court.

Our litigation experience spans a range of privacy issues. For example, we have defended clients in putative class actions alleging violations of federal and state credit reporting and health information privacy laws. We have also worked with clients that host e-mail to develop appropriate procedures to respond to subpoenas and other government requests for customer communications and information. Internationally, we have represented clients before the European national data protection authorities, and the Article 29 Working Party—a body representing the data protection Commissioners in the Member States of the European Union.

On the plaintiffs' side, we have won suits for violations of telemarketing and fax advertising rules, and have successfully challenged statutes and agency rules implicating privacy.

Charles E. Buffon
cbuffon@cov.com
202.662.5542

Erin M. Egan
eegan@cov.com
202.662.5145

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

REPRESENTATIVE MATTERS

- Represented a consortium of financial institutions in successfully challenging a California statute based on preemption by the Fair Credit Reporting Act (FCRA) of state and local laws limiting the exchange of customer information between affiliates.
- Successfully challenged as preempted a California statute that would have effectively overruled the federal Junk Fax Prevention Act with respect to interstate faxes.
- Represented Wyeth in a consumer class action alleging that it violated various privacy rights granted by the California Constitution, the California Confidentiality of Medical Information Act, and common law through its participation in direct mailing programs run by various pharmacies.
- Involved in several litigations over the constitutionality of security pat-downs at National Football League games.
- Advised a large pharmaceutical company in connection with litigation involving the alleged infringement of patient privacy by a pharmacy chain that collects personal information about prescription drug users.
- Successfully sued a major sender of "junk faxes" for violating the Telephone Consumer Protection Act and the Federal Communications Commission's rules on fax advertising.
- Successfully challenged before the DC Circuit the Federal Communication Commission's rules mandating that telecommunications companies install equipment to monitor private telephone and Internet communications.
- Represented Microsoft before the Article 29 Working Party on alleged violations of data protection rules.

TRANSACTIONAL

Privacy rules are often implicated during the sale or purchase of a business asset, such as customer databases or client lists that contain personal data; the acquisition or divestiture of a business that involves employee information; business restructurings that materially alter how an organization processes customer or staff information; and due diligence exercises involving the disclosure of personal information. In each of these circumstances, Covington's global privacy and data security lawyers draw upon their expertise to ensure that the transfer of personal information is effected in accordance with applicable laws, regulations, and recommended practices. We also closely examine the underlying privacy policies and practices of the entities involved to confirm both that data is handled in accordance with such policies, and that the policies themselves meet appropriate standards and are consistent with the transaction's objectives.

Erin M. Egan
eegan@cov.com
202.662.5145

Henriette Tielemans
htielemans@cov.com
32.2.549.5252

Lee J. Tiedrich
ltiedrich@cov.com
202.662.5403

We are involved throughout the transactional process to ensure that documentation adequately addresses relevant privacy issues, including contractual rights and limitations governing the ownership, collection, use, distribution, and security of personal and aggregate information. We regularly craft confidentiality agreements, security protocols, transfer agreements, and related policies for data rooms (both online and off-line), and we also attend to various post-transaction privacy-related tasks. In addition, we offer continuing transactional advice to clients as they grow and expand their business. In this regard, we often prepare notices, consent forms, disclosure documents, vendor contracts, transfer documents, certification documents under the US-European Union (EU) Safe Harbor regime, and other agreements in the context of employment or third party relationships.

REPRESENTATIVE MATTERS

- Handled the data privacy implications arising from the acquisition of an EU pharmaceutical company by a US-based company, including restructuring intra-company data flows following the transaction.
- Conducted due diligence regarding a target company's privacy and data security practices on behalf of a client seeking to acquire a healthcare information products company.
- Negotiated and drafted content-sharing agreements to acquire news and other content for a health-oriented website.
- Assisted several multinational companies fulfill their registration and notification obligations in multiple jurisdictions, including numerous European countries.