Privacy, E-Commerce, and Data Security

W. Gregory Voss
Katherine Woodcock
David Dumont
Nicholas D. Wells
Jonathan I. Exor

See next page for additional authors

Recommended Citation
https://scholar.smu.edu/til/vol46/iss1/8

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
Privacy, E-Commerce, and Data Security

Authors
W. Gregory Voss, Katherine Woodcock, David Dumont, Nicholas D. Wells, Jonathan I. Exor, João Luís Traça, Bernardo Embry, and Fatima Khan

This article is available in International Lawyer: https://scholar.smu.edu/til/vol46/iss1/8
Privacy, E-Commerce, and Data Security

W. Gregory Voss, Katherine Woodcock, David Dumont, Nicholas D. Wells, Jonathan I. Exor, João Luís Traca, Bernardo Embry, and Fatima Khan

This article reviews important legal developments during 2011 in the fields of privacy, e-commerce, and data security.¹

I. Developments in Europe

A. France

1. Legislative Developments

A new French law, referred to as “LOPPSI 2,”² was adopted on March 14, 2011. LOPPSI 2 makes online identity theft a crime, punishable under the new Article 226-4-1 of the French Criminal Code by one year in prison and a €15,000 fine,³ thus filling a void in French criminal law. LOPPSI 2 allows public authorities to use “video protection” in certain new cases, such as regulating traffic flows, prevention in areas particularly exposed to drug or other illegal trafficking, and preventing natural or technological risks, subject to the control of the Commission nationale de l’informatique et des libertés (CNIL), France’s

* The committee editor was W. Gregory Voss, Professor of Business Law, Toulouse University – Toulouse Business School, Toulouse, France, Attorney-at-Law, Avocat à la Cour. The authors were (Europe section): (France) W. Gregory Voss, (European Union) Katherine Woodcock and David Dumont, Lorenz International Lawyers, Brussels, Belgium. LaDawn Burnett, a student at Notre Dame Law School, assisted with the European Union section.

1. For earlier developments in this field, see Nicholas D. Wells, Poorvi Chothani & James M. Thurman, Information Services, Technology, and Data Protection, 44 INT'L LAW. 355 (2010).


3. Law 2011-267 of Mar. 14, 2011, art. 2 (Fr.).
data protection authority.4 A National Video Protection Commission prepares annual reports on the efficiency of video protection measures and makes recommendations.5

France implemented the “Telecoms Package” on August 26, 2011,6 amending Article 32, Chapter II of the French Data Protection Act to require information to be provided and consent obtained before cookies are placed.7 On October 26, 2011, the CNIL provided insight on what would be considered a cookie (e.g., “flash” cookies and local web storage), and to which cookies the rules do not apply (e.g., cookies used like a shopping cart on an e-commerce site, session ID cookies, or other cookies strictly necessary in order to provide requested services or content).8 A violation of the French Data Protection Act may cause the violator to incur fines of up to €300,000.9

2. Privacy

The CNIL was affected by the creation of a new French Defender of Rights (Défenseur des droits), which brought together previously dispersed defense of individual rights and liberties functions.10 For example, CNIL investigations are now subject to greater procedural controls, including in most cases, the right to be informed of the right to object.11

The CNIL exempted from declaration requirements data processing in the human resources and customer and prospect management areas carried out by French service providers on behalf of companies established outside of the European Union,12 although the latter must still comply with provisions of the French Data Protection Act such as data security.13 This measure facilitates outsourcing in France by non-European companies.14

Finally, the CNIL’s Sanction Committee determined on July 5, 2011, that the extraction of profiles from social networks by a website of the French Yellow Pages (Pages Jaunes) was an unfair data collection because (1) the data subjects were not previously informed, (2) the right to object was difficult to exercise, and (3) profiles were not effec-

4. Id. art. 18.
5. Id. art. 19.
7. Id. art. 37.
9. Id.
11. Id. art. 7.

VOL. 46, NO. 1
Social network terms and conditions of use providing that members’ personal data may be indexed by search engines did not apply because the website was not one. Yet *Pages Jaunes* received only a public warning because it had voluntarily ended its “web crawl” service in March 2011 after learning of a report proposing that it be sanctioned.16

### E-Commerce

The National Digital Council (CNNum—*Conseil national du numérique*) was established on April 29, 2011, to play an advisory role to the French government on the digital economy.17 The CNNum’s six-month report, issued on October 26, 2011, highlighted (1) the fact that digital economy represents only 3.2% of gross national product (GNP) in France compared to 5.4% in the United Kingdom, and (2) the need for greater competitiveness in that sector through higher education, more public and private financing of innovation, and more favorable taxation of young innovative companies.18

### B. EUROPEAN UNION

1. **EU Article 29 Data Protection Working Party (WP) Guidance**

   a. **Definition of Consent**

   The WP adopted its opinion on the definition of consent, and clarified the concept as currently applied in the Data Protection Directive19 and the e-Privacy Directive20 as a legal basis for processing personal data. First, consent means "... any indication of the [data subject’s] wishes ... signifying] his agreement...."21 There are no limits as to the form of consent, but some kind of affirmative action from the individual whose data is concerned (data subject) is required. Second, consent should be “freely given.”22
WP identifies situations and elements that can negatively affect this freedom of choice, particularly within the context of employment.\(^2\) Third, consent should be “specific,” referring to the exact purposes of the intended processing; blanket consent is not permitted, and specific consent clauses in contracts are required.\(^2\) Finally, the consent must be “informed.” The information provided should meet a certain quality standard,\(^2\) be clear, and sufficiently conspicuous to ensure that data subjects notice the information.

b. Online Behavioral Marketing

The WP published an open letter addressed to the Internet Advertising Bureau (IAB) Europe and the European Advertising Standards Alliance (EASA) on their draft self-regulatory “Framework for Online Behavioral Advertising” (the Code).\(^2\) The WP highlights that consent under the e-Privacy Directive is the same as the Data Protection Directive and that both standards should be applied consistently. They also highlight that the Code does not follow the EU standard of consent and that the Code (as is) does not fully comply with EU and various national laws.

c. Money Laundering and Terrorist Financing

The WP issued an opinion\(^2\) on the fundamental rights of privacy and anti-money-laundering and terrorist-financing obligations to strike a balance between the two, and annexed a list of forty-four different recommendations on the topic\(^2\)—varying from stipulating the possible legal bases for assessments, guidance on the proportionality principle, to policies and guidance on data retention. The main concepts from the recommendations are that privacy and data protection should be applied as a human right,\(^2\) and anti-money-laundering and terrorist-financing regulations should always have a clear legal basis and be necessary and proportionate to the personal data. Further, the obligations and principles should be approached “in a balanced way.”\(^2\) Finally, the WP suggests different means of “prior assessment,” such as privacy impact assessments, binding corporate rules, stress tests, benchmarking for adequacy of international transfers, etc.\(^2\) All of these

\(^{23}\) Id. at 13-14.

\(^{24}\) Id. at 17-18.

\(^{25}\) That is, “in plain text, without use of jargon,” and in understandable language. Id. at 20.


\(^{31}\) Id. at 4.
should be combined with continued and improved cooperation among stakeholders to ensure legal certainty in anti-money-laundering and terrorist financing.

d. Data Breach Framework

The WP working document on the data breach framework\textsuperscript{32} examined the current status of the framework under the e-Privacy Directive, and contemplated the inclusion of a harmonized framework in the Data Protection Directive. Focusing on the different approaches by Member States, the WP aims at harmonizing the approach within the EU by raising awareness of security breach procedures and coordination in instances of cross-border data breaches. The WP states that the existing data breach framework will be expanded beyond e-communications service providers to include all data controllers.

Finally, the WP recommends that the Commission issue guidance on data breaches and specifically include recommendations relating to: (1) circumstances when data breaches should be notified; (2) procedures to be followed in case of data breach; (3) a standard EU form for notifying data breaches; (4) the specific modalities for informing implicated individuals; (5) the information that should be kept and documented in case of data breach, and (6) technological protection measures that would allow an exemption from notification. The result of such recommendations is that there will be larger amounts of practical guidance at the EU level that allows for more harmonization throughout the EU.

e. Geolocation

The WP’s opinion on geolocation services on smart mobile devices sets out the legal framework that is applicable to such services provided and generated by smart mobile devices (Smart Devices).\textsuperscript{33} Location data from Smart Devices qualifies as personal data under the Data Protection Directive and telecom operators processing location data are also subject to the regulations of the e-Privacy Directive. Further, this Opinion identifies the main requirements that such companies have to satisfy.

They are required to obtain prior, free, specific, and informed opt-in consent of the data subject in most cases.\textsuperscript{34} Adequate notice of the processing of location data should be provided to the users of Smart Devices.\textsuperscript{35} Companies providing geolocation services or applications must give users access to the location data being processed that was collected from their Smart Devices.\textsuperscript{36} Finally, location data should be deleted (as well as created profiles based on such data) after a justified period of time because such data may only be kept for as long as it is necessary to provide the geolocation services requested by the user.\textsuperscript{37}


\textsuperscript{34} Id. at 13–14.

\textsuperscript{35} Id. at 17–18.

\textsuperscript{36} Id. at 18.

\textsuperscript{37} Id. at 19.
f. RFID Applications

The WP also issued an opinion on RFID applications that highlights the importance of RFID devices for business and industry, but emphasized concerns about the privacy impact. The opinion encourages industry to use privacy impact assessment (PIA) frameworks that data controllers should implement and conduct prior to deploying the devices and also make available to data protection authorities. The opinion also requires industry to submit a proposal for such a framework in order to identify the privacy risks related to the intended use of the RFID application, assess the everyday privacy risks resulting from carrying and using such a device, and clarify how such tags can be deactivated. The opinion is accompanied by an annex including the industry's draft PIA assessment framework to be implemented by August 11, 2011. The opinion further encourages the use of it and the related previous WP opinion by the industry to improve their proposal.

2. EU Google Street View Cases

a. Belgium

In April 2011, Belgian authorities began their investigation into Google Street View and its non-compliance with the privacy protection laws. The federal prosecutor offered Google a settlement of €150,000 in response to the internet giant's unauthorized collection of private data from unencrypted Wi-Fi networks. In November 2011, Google agreed to pay the settlement.

b. France

On March 17, 2011, the CNIL levied the first fine ever against Google for the improper gathering and storage of data collected through its Street View program. The relative severity of the fine—€100,000—reflected the seriousness of the offense and sanctioned Google's failure to cooperate with the CNIL's investigation. In addition to collecting and recording photographs, Street View also collected data transmitted by Wi-Fi.

42. Id.
networks such as IDs, passwords, log-in details, and email exchanges without data subject knowledge.\textsuperscript{46}

c. Germany

In March 2011, the Berlin State Supreme Court held that Google Street View is legal in Germany.\textsuperscript{47} The Court ruled against a German woman who sued Google alleging that Street View violates privacy and property rights. The Court held that it is legal to take photographs from street level, noted that Google automatically blurs faces and license plates, and in addition, it allows Germans to opt-out of the service and have their house obfuscated. Despite its landmark win, in April 2011, Google decided to cease recording street images in Germany.\textsuperscript{48}

d. The Netherlands

In April 2011, the Dutch Data Protection Authority (DPA) announced that it would levy a €1 million fine against Google after it found that Street View obtained address data collected from more than 3.6 million Wi-Fi routers.\textsuperscript{49} The DPA issued the penalty order against Google to force them to offer an opt-out procedure and to inform the general public of the option.\textsuperscript{50} and ruled that: (1) a MAC address in combination with the calculated location of the Wi-Fi router is personal data; (2) Google has to permanently erase the collected SSIDs (network names) of Wi-Fi routers; and (3) Google is obliged to offer users the option to opt-out so that they can effectively object to the processing of data on their Wi-Fi routers at all times and free of charge.

II. Developments in the United States\textsuperscript{*}

A. U.S. Federal Developments

In April 2011, Senators Kerry and McCain introduced a draft of the Commercial Privacy "Bill of Rights" Act of 2011.\textsuperscript{52} Among the data privacy-related bills currently under

\begin{itemize}
  \item \textsuperscript{46} Id.
  \item \textsuperscript{47} Cyrus Farivar, \textit{Berlin Court Rules Google Street View is Legal in Germany}, DW-WORLD.DE, (Mar. 21, 2011), http://www.dw-world.de/dw/article/0,,14929074,00.html.
  \item \textsuperscript{50} Press Release, Dutch Data Protection Authority, Google Announces Opt-out Option for Collection of Data about WiFi Routers (Nov. 15, 2011), http://www.dutchdpa.nl/Pages/en_pb_20111115_google.aspx.
  \item \textsuperscript{*} Authors (United States section): (U.S. Fed. and State Law Developments) Nicholas D. Wells, Principal of Wells IP Law, LLC, Salt Lake City, Utah, a solo practice focused on intellectual property, technology and data privacy law; (Children’s Privacy, Location Tracking, and Behavioral Tracking) Jonathan I. Ezor, Assistant Professor of Law and Director, Institute for Business, Law and Technology, Touro College Jacob D. Fuchsberg Law Center. Prof. Ezor wishes to thank Scott Richman for assistance in this section.
consideration by Congress, it is regarded as the most likely to be enacted.\textsuperscript{53} Under the Kerry-McCain bill, the FTC would promulgate rules and have enforcement authority similar to that of Data Protection Authorities currently acting in the EU. No private right of action is available to consumers under the bill.

Importantly, the Kerry-McCain bill would supersede conflicting state laws, except certain state laws related to health or financial data, fraud protection, or those that relate to data breach notification requirements, a subject that the Kerry-McCain bill does not address. Penalties under the bill are significant, with civil liability of $16,500 per offense, per day, up to $3 million.

But the Kerry-McCain bill lacks consumer protections, breach notification, and provisions related to online tracking of consumer activity. Several other congressional bills introduced in 2011 address these and other issues (e.g., the Do-Not-Track Online Act of 2011,\textsuperscript{54} the Do Not Track Me Online Act of 2011\textsuperscript{55}, and the BEST PRACTICES Act in 2011,\textsuperscript{56} which includes data privacy provisions but not a specific do-not-track provision).

Some bills introduced in 2011 include federal breach notification provisions, which many feel is needed to address the growing mesh of potentially conflicting state laws in this area. Notable among these are the Data Breach Notification Act of 2011\textsuperscript{57} and the discussion draft of the Secure and Fortify Electronic Data Act (the “SAFE Data Act”),\textsuperscript{58} which is focused on consumer protection and includes measures for both data security and data breach notification through both law enforcement agencies and the FTC but no private right of action for violations.

More extensive than either of the above bills is Senator Blumenthal’s Personal Data Protection and Breach Accountability Act of 2011,\textsuperscript{59} which, in case of a data breach, imposes written and telephonic notification obligations as well as public notice via media outlets for breaches involving more than 5,000 individuals.


\textsuperscript{58} SAFE Data Act, H.R. Res. 2577, 112th Cong. (2011), \url{http://www.opencongress.org/bill/112-h2577/text}.

In June 2011, Senator Leahy introduced his Personal Data Privacy and Security Act of 2011.60 This bill is broader in scope than the other pending data breach notification bills. The Leahy Bill, the Data Breach Notification Act of 2011, and the bill introduced by Senator Blumenthal were reported out of the Senate Judiciary Committee in September 2011 and may now be considered by the full Senate,61 although their eventual passage is uncertain.

B. U.S. STATE LAW DEVELOPMENTS

A bill amending California’s breach notification provisions was signed into law.62 It requires additional content in all breach notification letters to California residents.63 Any breach involving more than 500 California residents must be reported to the Attorney General of California.

California also joined seven other states that restrict public and private employers from using consumer credit reports to make hiring decisions.64 Credit reports may still be used for consideration of certain types of employees such as managerial positions or those involving access to confidential information or engaging in financial transactions.

In June 2011, Texas signed into law an expansive health privacy bill that imposes obligations in excess of those in the federal Health Insurance Portability and Accountability Act (HIPAA).65 The Texas bill expands the definition of “covered entity” as compared to HIPAA and requires employees of all covered entities to undergo training on both HIPAA and the new Texas law.66

Under the Texas bill, government agencies must develop “privacy and security standards for the electronic sharing of protected [personal] health information,” and the Texas Attorney General and other state departments are authorized to conduct compliance audits

---


63. Id.


of covered entities that have a history of violating the law.\textsuperscript{67} Expanded provisions related to data breach notification are under consideration in both Virginia\textsuperscript{68} and Oregon.\textsuperscript{69}

Several states are also considering legislations to address the risks created by electronic devices that may retain personal data.\textsuperscript{70} Of special concern are digital copiers, which have been shown to retain internal copies of documents that were copied or printed.\textsuperscript{71} Similar legislations are under consideration in Connecticut, Florida, Oregon, New Jersey, and Nevada.\textsuperscript{72}

C. CHILDREN’S PRIVACY, LOCATION TRACKING, AND BEHAVIORAL TRACKING

The year 2011 was a significant year in business privacy and data protection law in the United States. Legislatures, law enforcement bodies, and the courts have either addressed for the first time or revisited a number of key areas of relevant law, and those bodies appear likely to continue to do so into 2012. Among these issues are children’s privacy, location tracking, and behavioral tracking.

The major legal regime for protecting children’s personally identifiable information (PII) from improper collection, use, and disclosure is found in the Children’s Online Privacy Protection Act of 1998 (COPPA)\textsuperscript{73} and the accompanying regulations\textsuperscript{74} promulgated and enforced by the FTC. In 2011, the FTC continued its ongoing COPPA enforcement activity beyond web sites, and expanded it to the growing market for mobile applications (apps) intended for use by children under the age of thirteen. In May 2011, the FTC obtained a consent decree and order\textsuperscript{75} requiring the operators of twenty online worlds to pay a record $3 million penalty and substantially revise their practices after collecting PII from “hundreds of thousands of children under age 13 without their parents’ prior consent”\textsuperscript{76} as required by COPPA.\textsuperscript{77} In September, the FTC announced a consent decree


\textsuperscript{71} \textit{See, e.g.}, id.; \textit{Electronic Equipment Recycling and Reuse Act, N.Y. ENVTL. CONSERV. LAW §§ 27-2601, -2603(5)(b)-(c) (2010).} \textsuperscript{72} Hunton & Williams LLP, \textit{States Attempt to Address Privacy Risks Associated with Digital Copiers and Electronic Waste, supra note 70.}


and order,78 including a $50,000 settlement, against a developer whose apps (rather than a web site) targeted and collected PII from children.79 This new focus on apps parallels the FTC's call in the same month for public comments (due in late November 2011) on proposed revisions to its COPPA regulations, addressing both changes in technology and how children utilize the Internet.80

As many more consumers adopted devices such as smartphones81 with built-in global positioning system (GPS) features, the ability of companies and governmental entities alike to remotely track their locations drew legal scrutiny. At a May 10, 2011, hearing of the Senate Judiciary Committee's Subcommittee on Privacy, Technology and the Law82 officials from mobile technology leaders Apple and Google—along with representatives from the FTC, the Department of Justice, industry, and watchdog groups—testified as to the current and potential uses of location tracking technology. Increased tracking by mobile devices, as well as by social networks including Facebook,83 have led to the introduction of the Location Privacy Protection Act of 2011,84 which is currently being considered by Congress. In the courts, consumers brought lawsuits against Microsoft,85 Apple,86 and Google87 over their location-tracking and disclosure practices, and the United States Supreme Court heard arguments in United States v. Jones88 to consider whether warrantless law enforcement GPS monitoring of an individual's car violates the Fourth Amendment of the U.S. Constitution.

Throughout 2011, behavioral tracking—through which companies may identify and collect information on users' access across multiple web sites—remained the focus of legislative and other attention. At least two relevant bills—the Commercial Privacy Bill of Rights Act89 and the Do-Not-Track Online Act of 201190—were introduced and are currently being considered by congressional committees. California also introduced its own

do not-track bill. Consumers brought anti-tracking lawsuits against several companies, including, analytics firms ComScore and KISSmetrics, while social network leader Facebook faced multiple lawsuits over its ability to track its users even after they have “logged out” of the Facebook site itself. As the law evolves, so too does the enabling technology. The World Wide Web Consortium (W3C), the independent organization that sets standards for web-based communication, is working with the major browser publishers (Mozilla, Google, and Microsoft) and others to enable greater user control of whether and how behavior can be tracked.

While children’s privacy is the subject of formal federal statutory and regulatory requirements, for now, location and behavior tracking remain largely subject to self-regulation, although Congress, state legislatures, and the courts are all paying increasing attention to them. As the technologies and potential uses (and abuses) continue to evolve, so too can the legal environment be expected to develop and adapt.

III. Developments in Angola*

Earlier this year, the Angolan Parliament enacted a new Data Protection Act (DPA). This marks the first effort by the Angolan legislature to address the processing of personal data by both public and private entities in Angola. The framework laid down by the DPA is strongly inspired by, and follows the same basic principles as, the EU Data Protection Directive. The DPA further addresses issues that are regulated piecemeal by other European directives, such as the use of personal data for the purposes of sending advertising by e-mail or post.

---

93. See id.; Sebastian Anthony, AOL, Spotify, GigaOm, Etsy, KISSmetrics Sued Over Undeletable Tracking Cookies, EXTREME TECH (Aug. 4, 2011, 7:07 AM), http://www.extremetech.com/internet/91966-aol-spotify-gigaom-etsy-kissmetrics-sued-over-undeletable-tracking-cookies. The class action plaintiffs have also sued KISSmetrics’s clients including Spotify, Etsy, and others.
* Authors (Angola): João Luís Traça, Partner in charge of the Data Protection practice, admitted to the Portuguese Bar, and Bernardo Embry, a junior associate admitted to the Bar of England and Wales as a non-practicing barrister, Miranda, Correia, Amendoeira & Associados, Lisbon, Portugal.
96. See generally Lei No. 22/11, de 17 de Junho de 2011 – Da Proteccao de Dados Pessoais (Angola).
97. Previously, the issue of privacy in Angola had been governed by a number of disparate provisions of constitutional, tort, and employment law. See, e.g., 2010 C.F. art. 69 (Angola); Angolan Civil Code, art. 80; Law No. 8/04 of Nov. 1, 2004, art. 13(1); Law No. 2/00 of Feb. 11, 2000, art. 285.
The DPA concerns only the processing of personal data that has some connection with the Angolan territory: namely, where data are processed by a data controller based in Angola, or by a data controller located outside of Angola through any means located in Angolan territory. In the latter case, the DPA stipulates that a data controller will be considered to use “means” located in Angola whenever such means are used for collection, storage, or registration purposes, or even merely to transfer the data elsewhere.\textsuperscript{100} It follows that whenever a foreign entity sends personal data to Angola—even for storage in a data center—this transfer and the foreign transferor entity will be subject to the DPA, regardless of whether the data relates to Angolan nationals.

For the purposes of this statute, “personal data” is defined in almost identical terms to the definition provided by the Portuguese-language version of the Data Protection Directive. But, because the DPA definition of “personal data” only covers information relating to natural persons, the DPA does not apply to corporate data.\textsuperscript{101} Data subjects have the right to be informed about their personal data, and they can access, correct, and update the information.\textsuperscript{102}

Following best international practices, personal data may be classified as relating to health and sex life, creditworthiness and solvency, unlawful activities, or “sensitive data.” This last category encompasses all personal data on an individual’s philosophical or political convictions, union or political party affiliation, faith, private life, and racial or ethnic origin.\textsuperscript{103} Personal data that do not fall into one of the specific categories provided for by the DPA are dealt with under the generic heading of “personal data,” and are subject to general procedural requirements and guarantees.

Refusing to adopt a “one size fits all” approach to personal data processing, the Angolan legislature defined different legal requirements for the various data processing operations based on the type of data concerned and the processing objectives. Compliance with the regime must be assessed on a case-by-case basis, taking into account the specific content and circumstances of each operation. Besides differentiating between various types of data, the DPA also imposes special requirements where personal data are to be used for the purposes of sending marketing communications, and where the data are collected for surveillance purposes, including for the recording of telephone calls.\textsuperscript{104}

All data processing operations must be registered with the regulatory authority. Operations that involve only the processing of generic data are only subject to notification.\textsuperscript{105} Operations involving any of the specific categories of personal data referred to above require prior authorization by the regulator.\textsuperscript{106} Similarly, using personal data to send marketing communications involves only a notification, while recording phone calls or data for surveillance purposes requires prior authorization. The difference between notification and prior authorization is mostly procedural. Notification involves submitting the relevant forms and documents to the regulatory body, while data processing may commence thirty days thereafter unless the regulator decides otherwise during this period. If a

\begin{flushright}
\textsuperscript{100}. See Lei No. 22/11, de 17 de Junho de 2011 - Da Proteccao de Dados Pessoais, art. 3 (Angola).
\textsuperscript{101}. See id. arts. 26, 28.
\textsuperscript{102}. See id. art. 5(b).
\textsuperscript{103}. See id. art. 5(c).
\textsuperscript{104}. See id. arts. 13-16.
\end{flushright}
prior authorization is required, no data processing may take place until such authorization is obtained. The DPA does not set a timeframe for the authorization to be issued.\textsuperscript{107}

The transfer of personal data to outside of Angola is subject to particular rules that differ depending on whether the destination country offers an adequate level of protection. The Angolan regulator compares the destination country's data protection legislation to the DPA. All data transfers abroad must be registered; however if the destination country does not offer an adequate level of protection, a prior authorization must be obtained, but is only available in limited cases. These cases include when the written consent of the data subject has been obtained or when the exportation is necessary for contract performance.\textsuperscript{108}

The DPA calls for the creation of an Angolan Data Protection Agency that will receive notifications and issue authorizations for data processing. It will also keep a public register of all data processing operations carried out in Angola and monitor compliance with the DPA.\textsuperscript{109} Although the Angolan Data Protection Agency does not exist yet, the DPA is immediately enforceable. Therefore, actions (both administrative and judicial) can be brought to obtain relief if the DPA is breached. All entities that fall under the DPA should comply with its terms as from now, except where the Angolan Data Protection Agency is involved. Failure to do so may lead to stiff penalties, including fines of up to $150,000 and a jail term of up to three years in case of a serious breach.\textsuperscript{110}

IV. Developments in Online Dispute Resolution and Its Relationship with E-Commerce*

A. ONLINE DISPUTE RESOLUTION AND E-COMMERCE

Online dispute resolution (ODR) provides a mechanism for redress that helps to increase consumer trust, thereby stimulating the growth of e-commerce. ODR is primarily made up of alternative dispute resolution processes enabled or assisted by information and communications technology.\textsuperscript{111} An ODR proceeding typically includes an online-based process that is low-cost and efficient, similar to an e-commerce transaction. Having noticed these benefits, companies have embraced ODR technologies for the successful and cost-effective resolution of disputes online.\textsuperscript{112} The United Nations Commission on Inter-

\textsuperscript{107} See id. art. 35 (giving a timeframe only for notification).
\textsuperscript{108} See id. art. 23. No statutory guidance is given as to how this comparison should be carried out, or as to the criteria that should be used.
\textsuperscript{109} See id. art. 44(a), (g).
\textsuperscript{110} See id. arts. 49, 56-57.
\textsuperscript{*} Author (Developments in Online Dispute Resolution and Its Relationship with E-Commerce): Fatima Khan, Principal of Fatima Khan Consulting, Houston, Texas.
\textsuperscript{111} See Pablo Cortés, ONLINE DISPUTE RESOLUTION FOR CONSUMERS IN THE EUROPEAN UNION (2011); see generally Ethan Katsh, Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace, 10 LEX ELECTRONICA 3 (2006), available at http://www.lex-electronica.org/docs/articles_65.pdf (discussing the evolution of ODR).
\textsuperscript{112} See, e.g., infra notes 118-21.
national Trade Law (UNCITRAL) Working Group III (WG.III) has also developed and is considering draft generic model rules on ODR.\textsuperscript{113} Traditionally, consumers have proceeded cautiously before engaging in cross-border e-commerce transactions because there is often no mechanism for redress if the transaction fails.\textsuperscript{114} ODR remedies this problem by supplying "consumers and businesses with trust and consistency in the resolution of disputes" by increasing consumer confidence, leading to the growth of e-commerce.\textsuperscript{115}

Companies and governments around the world have increasingly adopted ODR as a viable solution to resolve both e-commerce and offline disputes.\textsuperscript{116} For example, eBay employs SquareTrade for disputes arising out of eBay transactions.\textsuperscript{117} eBay has a caseload of over 60 million per year, with 30 million resolved amicably in-house.\textsuperscript{118} Also, General Electric has employed Cybersettle and has settled fifteen disputes over claims for a total of €136,000 during a three-month trial period in 2011.\textsuperscript{119} In Mexico, Concilianet, a service provided by the Federal Attorney's Office of the Consumer, provides conciliation and arbitration services to resolve business-to-consumer (B2C) disputes.\textsuperscript{120} In Europe, the European Commission recently proposed a regulation on consumer ODR and announced its intention to create a European Community-wide single online platform to resolve contractual disputes within thirty days.\textsuperscript{121} The year 2011 gave rise to new ODR providers that have taken different approaches to dispute resolution, showing that the market is responding to a need for ODR.\textsuperscript{122} One such company, ZipCourt, closely follows the UNCITRAL draft model rules and allows disputants to participate in an ODR proceeding tailored to the dispute.\textsuperscript{123} Another company, Modria, offers ODR products and services.\textsuperscript{124}

---


\textsuperscript{114} See Which? Survey Reveals Online Shopping Fears, WHICH NEWS (Nov. 23, 2011), http://www.which.co.uk/news/2011/11/which-survey-reveals-online-shopping-fears-272262/ (discussing a survey of British public that revealed that "50% of online shoppers would rather use a British website even if the product was cheaper from an EU one").

\textsuperscript{115} See Cortés, supra note 111, at 2.


B. UNCITRAL

In mid-2011, UNCITRAL reaffirmed WG.III’s mandate to address ODR relating to cross-border electronic transactions.\textsuperscript{125} WG.III has created draft generic procedural rules on ODR to apply to both business-to-business (B2B) and B2C transactions, which are under consideration.\textsuperscript{126}

The UNCITRAL model rules put forth a three-stage proceeding: negotiation, facilitated settlement, and arbitration.\textsuperscript{127} First, the parties may choose to negotiate the claim and reach a solution.\textsuperscript{128} If parties fail to do so, the process moves into the facilitated settlement stage.\textsuperscript{129} Similarly, if the parties fail to reach an agreement during facilitated settlement, the process moves into arbitration.\textsuperscript{130} During recent sessions, WG.III discussed the three-stage design and disputants’ options to participate in each stage.

During its May 2011 session, WG.III discussed a number of other issues as well, including the ODR framework, proceeding, providers and platforms, neutral selection, and enforceability under the New York Convention.\textsuperscript{131} Currently, UNCITRAL continues to develop and discuss the draft model rules, having held its most recent session in November 2011.\textsuperscript{132}

\begin{footnotes}
\item 126. See id. The draft generic procedural rules discussed do not reflect the changes made during the WG.III's 3rd meeting in November 2011.
\item 127. See id. at 3.
\item 128. See id. at 13.
\item 129. See id.
\item 130. See id. at 18.
\end{footnotes}