الفصل الرابع

من سلسلة محاضرات لمساق

أخلاقيات المهنة في تكنولوجيا المعلومات

د. محمد فوزي العقاد

Chapter 4
PRIVACY

Learning Objectives

As you read this chapter, consider the following questions:

- What is the right of privacy, and what is the basis for protecting personal privacy under the law?
- What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?
- What are the various strategies for consumer profiling, and what are the associated ethical issues?
- What is e-discovery, and how is it being used?
- Why and how are employers increasingly using workplace monitoring?
- What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

ما هو حق الخصوصية ، وما أساس حماية الخصوصية الشخصية بموجب القانون؟

ما هي بعض القوانين التي توفر حماية البيانات الشخصية، وما هي بعض القضايا الأخلاقية المرتبطة بها؟

ما هي الاستراتيجيات المختلفة لتصنيف المستهلك ، وما هي القضايا الأخلاقية المرتبطة بها؟

ما هو الاكتشاف الإلكتروني وكيف يتم استخدامه؟

لماذا وكيف يستخدم أصحاب العمل بشكل متزايد مراقبة مكان العمل؟

ما هي قدرات تقنيات المراقبة المتقدمة ، وما هي القضايا الأخلاقية التي تثيرها؟

Organizations Behaving Badly المنظمات التي تتصرف بشكل سيء

WhatsApp, an instant messaging app for smartphones, allows users to send text messages, documents, images, videos, user location data, and other data over the Internet to other WhatsApp users, using standard cellular mobile numbers. In the past, WhatsApp has been a strong defender of its users' privacy, employing end-to-end encryption for all messages sent through its service and regularly resisting requests from authorities for data access. As a result, WhatsApp has been the instant messaging app of choice for users who wish to keep their conversations private, including individuals working to expose corruption within organizations and those reporting on the activities of totalitarian governments.

يتيح تطبيق WhatsApp، وهو تطبيق مراسلة فورية للهواتف الذكية ، للمستخدمين إرسال رسائل نصية ومستندات وصور ومقاطع فيديو وبيانات موقع المستخدم وبيانات أخرى عبر الإنترنت إلى مستخدمي WhatsAppالآخرين ، باستخدام أرقام الهواتف المحمولة. في الماضي ، كان WhatsAppمدافعًا قويًا عن خصوصية مستخدميه ، حيث يستخدم التشفير من طرف إلى طرف لجميع الرسائل المرسلة من خلال خدمته ويقاوم بانتظام طلبات السلطات للوصول إلى البيانات. نتيجة لذلك ، كان WhatsAppهو تطبيق المراسلة الفورية المفضل للمستخدمين الذين يرغبون في الحفاظ على خصوصية محادثاتهم ، بما في ذلك الأفراد الذين يعملون على كشف الفساد داخل المنظمات وأولئك الذين يقومون بالإبلاغ عن أنشطة الحكومات الشمولية.

Organizations Behaving Badly

Facebook purchased WhatsApp for $22 billion in 2014. After the sale to Facebook was announced, WhatsApp CEO and cofounder Jan Koum declared that nothing would change with the company's privacy practices. Indeed, Koum posted that "If partnering with Facebook meant that we had to change our values, we wouldn't have done it." This statement has come back to haunt him. In the fall of 2016, WhatsApp announced that it would begin providing user data—including phone numbers, usage data, and information on devices and operating systems being used—to Facebook and the "Facebook family of companies." According to the company, this information allows Facebook to make better friend suggestions and display more relevant ads to users while also allowing businesses to send messages to users, including appointment reminders, delivery and shipping notifications, and marketing pitches. The policy shift is intended to help WhatsApp generate more revenue and makes economic sense; however, the change has raised concerns over the privacy of users' conversations and identities and has upset users drawn to the app by the company's previous strong stance on privacy. What trade-offs should social network organizations consider when changing their privacy policy? Must the scales always be tipped in favor of increased revenue?

في عام 2014 قامت شركة فيسبوك بشراء WhatsApp مقابل 22 مليار دولار. بعد الإعلان عن البيع إلى Facebook، أعلن الرئيس التنفيذي لشركة WhatsAppوالشريك المؤسس جان كوم أنه لن يتغير شيء مع ممارسات الخصوصية للشركة. في الواقع ، نشر كوم أنه "إذا كانت الشراكة مع Facebookتعني أنه يتعين علينا تغيير قيمنا ، لما فعلنا ذلك." عاد هذا البيان ليطارده. في خريف عام 2016 ، أعلنت WhatsAppأنها ستبدأ في تقديم بيانات المستخدم - بما في ذلك أرقام الهواتف وبياناتِ الاستخدام والمعلومات المتعلقة بالأجهزة وأنظمة التشغيل المستخدمة - إلى Facebookو "مجموعة شركات Facebook".وفقًا للشركة ، تسمح هذه المعلومات لـ Facebookبتقديم اقتراحات صداقة أفضل وعرض إعلانات أكثر صلة للمستخدمين مع السماح أيضًا للشركات بإرسال رسائل إلى المستخدمين ، بما في ذلك تذكيرات المواعيد ، وإشعارات التسليم والشحن ، وملاعب التسويق. يهدف التحول في السياسة إلى مساعدة WhatsAppفي تحقيق المزيد من الإيرادات وجعلها منطقية من الناحية الاقتصادية ؛ ومع ذلك ، أثار التغيير مخاوف بشأن خصوصية محادثات المستخدمين وهوياتهم وأزعج المستخدمين الذين انجذبوا إلى التطبيق بسبب الموقف القوي السابق للشركة بشأن الخصوصية. ما المفاضلات التي يجب على مؤسسات الشبكات الاجتماعية مراعاتها عند تغيير سياسة الخصوصية الخاصة بها؟ هل يجب أن تميل الموازين دائمًا لصالح زيادة الإيرادات؟

Privacy Protection and the Law حماية الخصوصية والقانون

The use of information technology in both government and business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used. Information about people is gathered, stored, analyzed, and reported because organizations can use it to make better decisions (see Figure 4-1). Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship, can profoundly affect people's lives. In addition, the global marketplace and intensified competition have increased the importance of knowing consumers' purchasing habits and financial condition. Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services. Organizations also need basic information about customers to serve them better. It is hard to imagine an organization having productive relationships with its customers without having data about them. Thus, organizations want systems that collect and store key data from every interaction they have with a customer.

يتطلب استخدام تكنولوجيا المعلومات في كل من الحكومة والشركات تحقيق التوازن بين احتياجات أولئك الذين يستخدمون المعلومات التي يتم جمعها مقابل حقوق ورغبات الأشخاص الذين يتم استخدام معلوماتهم. يتم جمع المعلومات حول الأشخاص وتخزينها وتحليلها والإبلاغ عنها لأن المنظمات يمكن أن تستخدمها لاتخاذ قرارات أفضل (انظر الشكل 4-1). يمكن لبعض هذه القرارات ، بما في ذلك تعيين مرشح وظيفة أو الموافقة على قرض أو تقديم منحة دراسية أو عدم تعيينها ، أن تؤثر بشكل كبير على حياة الناس. بالإضافة إلى ذلك ، أدى السوق العالمي والمنافسة الشديدة إلى زيادة أهمية معرفة العادات الشرائية للمستهلكين ووضعهم المالي. تستخدم الشركات هذه المعلومات لتوجيه جهود التسويق إلى المستهلكين الذين من المرجح أن يشتروا منتجاتهم وخدماتهم. تحتاج المنظمات أيضًا إلى معلومات أساسية حول العملاء لخدمتهم بشكل أفضل. من الصعب تخيل وجود منظمة علاقات مثمرة مع عملائها دون وجود بيانات عنهم. وبالتالي ، تريد المؤسسات أنظمة تجمع البيانات الأساسية وتخزنها من كل تفاعل لها مع العميل.

FIGURE 4-1 Organizations gather a variety of data about people in order to make better decisions

Privacy Protection and the Law

Systems collect and store key data from every interaction with customers to make better decisions. Many object to data collection policies of government and business Privacy Key concern of Internet users .

Top reason why nonusers still avoid the Internet Reasonable limits must be set Historical perspective on the right to privacy Fourth Amendment reasonable expectation of privacy.

تقوم الأنظمة بجمع وتخزين البيانات الرئيسية من كل من تفاعل معها من العملاء لاتخاذ قرارات أفضل. يعترض الكثيرون على سياسات جمع البيانات الحكومية وخصوصية الشركات ويعتبر ذلك مصدر قلق رئيسي لمستخدمي الإنترنت.

الاسباب الرئيسية لتجنب البعض لاستخدام الانترنت. الالتزام بقيود منطقية يجب تحديدها. وجهة نظر تاريخية تتعلق بالخصوصية. التعديل الرابع لاتفاقية الخصوصية الشخصية

Information Privacy

Information Privacy A broad definition of the right of privacy is “the right to be left alone—the most comprehensive of rights, and the right most valued by a free people.” Another concept of privacy that is particularly useful in discussing the impact of IT on privacy is the term information privacy, first coined by Roger Clarke, director of the Australian Privacy Foundation. Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one’s personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and their use). The following sections cover concepts and principles related to information privacy, beginning with a summary of the most significant privacy laws, their applications, and related court rulings.

خصوصية المعلومات: إن التعريف الواسع للحق في الخصوصية هو الحق في أن يُترك الشخص بمفرده أكثر الحقوق شمولاً ، والحق الأكثر تقديرًا من قبل الأشخاص الأحرار.

مفهوم آخر للخصوصية مفيد بشكل خاص في مناقشة تأثير تكنولوجيا المعلومات على الخصوصية هو مصطلح خصوصية المعلومات ، الذي صاغه لأول مرة روجر كلارك ، مدير مؤسسة الخصوصية الأسترالية. حيث عرف خصوصية المعلومات بأنها (مزيج من خصوصية الاتصالات والقدرة على التواصل مع الآخرين دون مراقبة هذه الاتصالات من قبل أشخاص أو منظمات أخرى) وخصوصية البيانات (القدرة على تقييد الوصول إلى البيانات الشخصية للفرد من قبل الأفراد والمؤسسات الأخرى من أجل ممارسة مهمة كبيرة. درجة التحكم في تلك البيانات واستخدامها).

تغطي الأقسام التالية المفاهيم والمبادئ المتعلقة بخصوصية المعلومات ، بدءًا من ملخص لأهم قوانين الخصوصية وتطبيقاتها وأحكام المحاكم ذات الصلة.

Privacy Laws, Applications, and Court Rulings
قوانين الخصوصية والتطبيقات وأحكام المحاكم

This section outlines a number of legislative acts that affect a person's privacy. Note that most of these actions address invasion of privacy by the government. Legislation that protects people from data privacy abuses by corporations is almost nonexistent. Although a number of independent laws and acts have been implemented over time, no single, overarching national data privacy policy has been developed in the United States. Nor is there an established advisory agency that recommends acceptable privacy practices to businesses. Instead, there are laws that address potential abuses by the government, with little or no restrictions for private industry. As a result, existing legislation is sometimes inconsistent or even conflicting. You can track the status of privacy legislation in the United States at the Electronic Privacy Information Center's website (www.epic.org). The discussion is divided into the following topics: financial data, health information, children's personal data, electronic surveillance, fair information practices, and access to government records.

يوضح هذا القسم عددًا من القوانين التشريعية التي تؤثر على خصوصية الشخص. لاحظ أن معظم هذه الإجراءات تتناول انتهاك الحكومة للخصوصية. لاحظ ان التشريعات التي تحمي الأشخاص من انتهاكات خصوصية البيانات من قبل الشركات تكاد تكون معدومة وذلك على الرغم من تنفيذ عدد من القوانين والأفعال المستقلة بمرور الوقت ، لم يتم تطوير سياسة خصوصية بيانات وطنية واحدة وشاملة في الولايات المتحدة. كما لا توجد وكالة استشارية راسخة توصي بممارسات خصوصية مقبولة للشركات. بدلاً من ذلك ، هناك قوانين تعالج الانتهاكات المحتملة من قبل الحكومة ، مع قيود قليلة أو معدومة على الصناعة الخاصة. ونتيجة لذلك ، فإن التشريعات الحالية غير متسقة أو حتى متضاربة في بعض الأحيان. يمكنك تتبع حالة تشريع الخصوصية في الولايات المتحدة على موقع ويب مركز معلومات الخصوصية الإلكتروني (www.epic.org).

حيث سيتم مناقشة الموضوعات التالية: البيانات المالية ، والمعلومات الصحية ، وبيانات الأطفال الشخصية ، والمراقبة الإلكترونية ، وممارسات المعلومات العادلة ، والوصول إلى السجلات الحكومية.

Financial Data

Legislative acts passed over the past 40 years. Most address invasion of privacy by the government No protection of data privacy abuses by corporations. No single, overarching national data privacy policy..

Financial Data Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts. To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN. The inadvertent loss or disclosure of these personal financial data carries a high risk of loss of privacy and potential financial loss. Individuals should be concerned about how these personal data are protected by businesses and other organizations and whether or not they are shared with other people or companies. Fair Credit Reporting Act (1970)

The Fair Credit Reporting Act (15 U.S.C. § 1681) regulates the operations of credit reporting bureaus, including how they collect, store, and use credit information. The act, enforced by the U.S. Federal Trade Commission, is designed to ensure the accuracy, fairness, and privacy of information gathered by the credit reporting companies and to provide guidelines for organizations whose systems that gather and sell information about people. The act outlines who may access your credit information, how you can find out what is in your file, how to dispute inaccurate data, and how long data are retained. It also prohibits a credit reporting bureau from giving out information about you to your employer or potential employer without your written consent.

القوانين التشريعية التي صدرت على مدى السنوات الأربعين الماضية. يتطرق معظمها إلى انتهاك الحكومة للخصوصية. لا توجد حماية لانتهاكات خصوصية البيانات من قبل الشركات. لا توجد سياسة خصوصية بيانات وطنية واحدة وشاملة ..

هناك مشكلة كبيرة تتمثل في انه يجب على الأفراد الكشف عن الكثير من بياناتهم المالية الشخصية من أجل الاستفادة من مجموعة واسعة من المنتجات والخدمات المالية المتاحة ، بما في ذلك بطاقات الائتمان وحسابات التحقق والادخار والقروض وإيداع الرواتب المباشر وحسابات الوساطة. للوصول إلى العديد من هذه المنتجات والخدمات المالية ، يجب على الأفراد استخدام اسم تسجيل الدخول الشخصي أو كلمة المرور أو رقم الحساب أو PIN. ينطوي الخسارة أو الإفشاء غير المقصود لهذه البيانات المالية الشخصية على مخاطر عالية تتمثل في فقدان الخصوصية والخسارة المالية المحتملة. يجب أن يشعر الأفراد بالقلق بشأن كيفية حماية هذه البيانات الشخصية من قبل الشركات والمؤسسات الأخرى وما إذا كانت تتم مشاركتها مع أشخاص أو شركات أخرى أم لا.

قانون الإبلاغ عن الائتمان العادل (1970)

ينظم قانون الإبلاغ عن الائتمان العادل (15 U.S.C. § 1681) عمليات مكاتب إعداد التقارير الائتمانية ، بما في ذلك كيفية جمع المعلومات الائتمانية وتخزينها واستخدامها. القانون الذي تفرضه لجنة التجارة الفيدرالية الأمريكية ، مصمم لضمان دقة وعدالة وخصوصية المعلومات التي تم جمعها من قبل شركات إعداد التقارير الائتمانية ولتوفير إرشادات للمنظمات التي تقوم أنظمتها بجمع وبيع معلومات عن الأشخاص. يحدد القانون من يمكنه الوصول إلى معلوماتك الائتمانية ، وكيف يمكنك معرفة ما هو موجود في ملفك ، وكيفية الاعتراض على البيانات غير الدقيقة ، ومدة الاحتفاظ بالبيانات. كما أنه يحظر على مكتب التقارير الائتمانية إعطاء معلومات عنك إلى صاحب العمل أو صاحب العمل المحتمل دون موافقتك الكتابية.

Financial data (cont’d.)

Gramm-Leach-Bliley Act (1999) Bank deregulation that enabled institutions to offer investment, commercial banking, and insurance services. Three key rules affecting personal privacy Financial Privacy Rule Safeguards Rule Pretexting Rule.

Opt-out policy Assumes that consumers approve of companies collecting and storing their personal information Requires consumers to actively opt out Favored by data collectors Opt-in policy Must obtain specific permission from consumers before collecting any data Favored by consumers.

قانون Gramm-Leach-Bliley (1999)

تنص مادة غرام-ليتش-بلايلي لسنة 1999 على تمكين المؤسسات من توفير خدمات بنكية تجارية وخدمات تامين، مع وجود ثلاث ضوابط رئيسية هي: الخصوصية المالية،ضوابط حماية، خدمات الاعلام المسبق.يفترض قانون الانسحاب ان يقوم العملاء مسبقا بالسماح للشركات بجمع بياناتهم الخاصة وفي حال عدم الموافقة يمكن للمستخدمين الانسحاب من الشركة، وينص قانون الاشتراك على ضرورة ان تحصل الشركة على اذن مسبق من المستخدم قبل الاشتراك في خدمات الشركة

Health Information معلومات صحية

The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread. Individuals are rightly concerned about the erosion of privacy of data concerning their health. They fear intrusions into their health data by employers, schools, insurance firms, law enforcement agencies and even marketing firms looking to promote their products and services. The primary law addressing these issues is the Health Insurance Portability and Accountability Act (HIPAA).

Health information Health Insurance Portability and Accountability Act (1996) Improves the portability and continuity of health insurance coverage Reduces fraud, waste, and abuse Simplifies the administration of health insurance American Recovery and Reinvestment Act (2009)Included strong privacy provisions for electronic health records Offers protection for victims of data breaches.

الان وعلى نطاق واسع جدا انتشر استخدام السجلات الطبية الإلكترونية مع ما يترتب على ذلك من ربط ونقل هذه المعلومات الإلكترونية بين المنظمات المختلفة.

الأفراد قلقون بحق بشأن تآكل خصوصية البيانات المتعلقة بصحتهم. إنهم يخشون التدخل في بياناتهم الصحية من قبل أرباب العمل والمدارس وشركات التأمين ووكالات إنفاذ القانون وحتى شركات التسويق التي تتطلع إلى الترويج لمنتجاتها وخدماتها.

القانون الأساسي الذي يعالج هذه القضايا هو قانون نقل التأمين الصحي والمساءلة .(HIPAA)

المادة الخاصة بالضمان والتامين الصحي لسنة 1996 تحسن من استمرارية ونجاعة شمولية التامين والخدمات الصحية وتقلل من المخاطر والاهدار و الاساءة وتبسط عملية ادارة التامين الصحي , كذلك المادة بالضمان والتامين الصحي لعام 2009 توفر خصوصية قوية للبيانات الرقيمة المتعلقة بالصحة وحماية الضحايا من مخاطر تسريب البيانات.

Privacy Laws, Applications, and Court Rulings

State laws related to security breach notification Over 40 states have enacted legislation requiring organizations to disclose security breaches. For some states, these laws are quite stringent. Children's personal data Children's Online Privacy Protection Act (1998)Web sites catering to children must offer comprehensive privacy policies, notify parents or guardians about its data-collection practices, and receive parental consent before collecting personal information from children under 13Family Education Rights and Privacy Act (1974)Assigns rights to parents regarding their children's education records Rights transfer to student once student becomes.

قوانين الولاية المتعلقة بإعلام الخرق الأمني: سنت أكثر من 40 ولاية تشريعات تطالب المنظمات بالكشف عن الانتهاكات الأمنية. حيث ان بعض الدول لديها القوانين صارمة للغاية فيما يتعلق ب.

البيانات الشخصية للأطفال والذي يكفله قانون حماية خصوصية الأطفال على الإنترنتر الصادر عام (1998) وبموجبة يجب أن تقدم مواقع الويب التي تلبي احتياجات الأطفال سياسات خصوصية شاملة ، وإخطار الوالدين أو الأوصياء بممارسات جمع البيانات ، والحصول على موافقة الوالدين قبل جمع المعلومات الشخصية من الأطفال دون سن 13 عامًا.

يخصص قانون الخصوصية وحقوق التعليم (1974) حقوقًا للآباء فيما يتعلق بسجلات تعليم أطفالهم. ونقل الحقوق إلى الطالب بمجرد أن يصبح الطالب بالغا.

Electronic surveillance المراقبة الالكترونية

Electronic Communications Privacy Act of 1986 (ECPA)Protects communications in transfer from sender to receiver Protects communications held in electronic storage Prohibits recording dialing, routing, addressing, and signaling information without a search warrant Pen register records electronic impulses to identify numbers dialed for outgoing calls Trap and trace records originating number of incoming calls.

قانون خصوصية الاتصالات الإلكترونية لعام 1986 (ECPA) يحمي الاتصالات أثناء النقل من المرسل إلى المستلم يحمي الاتصالات الموجودة في التخزين الإلكتروني يحظر تسجيل الاتصال والتوجيه والعنونة والإشارة إلى المعلومات دون أمر بحث يسجل سجل القلم النبضات الإلكترونية لتحديد الأرقام التي تم الاتصال بها للمكالمات الصادرة سجلات التتبع والتعقب التي تنشأ من عدد المكالمات الواردة.

Communications Assistance for Law Enforcement Act (CALEA) 1994Amended both the Wiretap Act and ECPA Required the telecommunications industry to build tools into its products so federal investigators could eavesdrop and intercept electronic communications Covered emerging technologies, such as: Wireless modems Radio-based electronic mail Cellular data networks.

المساعدة في الاتصالات لقانون إنفاذ القانون (CALEA)لعام 1994 تم تعديل كل من قانون التنصت على المكالمات الهاتفية وقانون حماية خصوصية الاتصالات الإلكترونية (ECPA)تطلبت صناعة الاتصالات السلكية واللاسلكية إنشاء أدوات في منتجاتها حتى يتمكن المحققون الفيدراليون من التنصت على الاتصالات الإلكترونية واعتراضها التقنيات الناشئة المغطاة ، مثل: أجهزة المودم اللاسلكية البريد الإلكتروني اللاسلكي الخلوي شبكات البيانات

USA PATRIOT Act (2001)Increased ability of law enforcement agencies to search telephone, , medical, financial, and other records Critics argue law removed many checks and balances that ensured law enforcement did not abuse its powers Relaxed requirements for National Security Letters (NSLs).

قانون باتريوت بالولايات المتحدة الأمريكية (2001) زيادة قدرة وكالات إنفاذ القانون على البحث في السجلات الهاتفية والطبية والمالية وغيرها من السجلات يجادل النقاد بأن القانون أزال العديد من الضوابط والتوازنات التي ضمنت أن تطبيق القانون لم يسيء استخدام صلاحياته المتطلبات المخففة لخطابات الأمن القومي ((NSL

Electronic surveillance المراقبة الالكترونية

Communications Act of 1934 Established the Federal Communications Commission Regulates all non-federal-government use of radio and television plus all interstate communications Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act)Regulates interception of telephone and oral communications Has been amended by new laws

Foreign Intelligence Surveillance Act (FISA) of 1978Describes procedures for electronic surveillance and collection of foreign intelligence information in communications between foreign powers and agents of foreign powers.

قانون الاتصالات لعام 1934: إنشاء لجنة الاتصالات الفيدرالية ينظم جميع استخدامات الحكومة غير الفيدرالية للراديو والتلفزيون بالإضافة إلى جميع الاتصالات بين الولايات. بقوانين جديدة

قانون مراقبة الاستخبارات الأجنبية (FISA)لعام 1978 يصف إجراءات المراقبة الإلكترونية وجمع معلومات الاستخبارات الأجنبية في الاتصالات بين القوى الأجنبية وعملاء القوى الأجنبية.

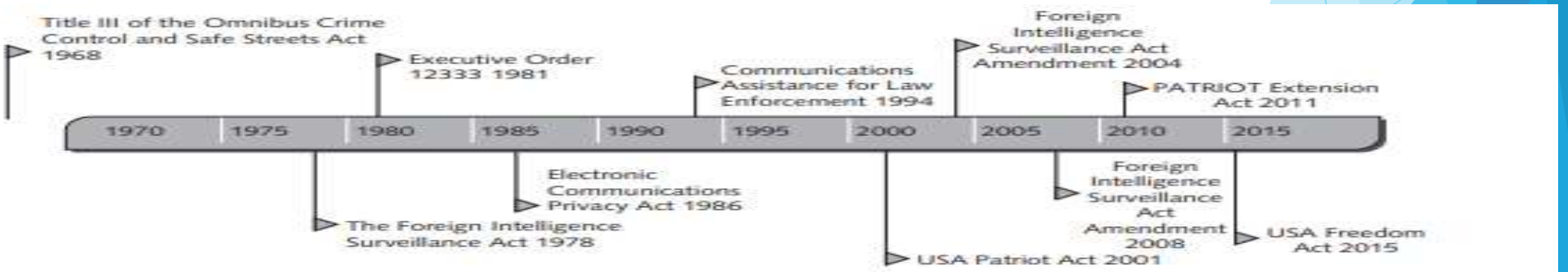

FIGURE 4-2 Various laws affecting electronic surveillance

Export of personal data تصدير البيانات الشخصية

Organization for Economic Co-operation and Development Fair Information Practices (1980)Fair Information Practices Set of eight principles Model of ethical treatment of consumer data.

ممارسات المعلومات العادلة لمنظمة التعاون الاقتصادي والتنمية (1980) مجموعة ممارسات المعلومات العادلة مجموعة من ثمانية مبادئ نموذج المعالجة الأخلاقية لبيانات المستهلك.

European Union Data Protection Directive. Requires companies doing business within the borders of 15 European nations to implement a set of privacy directives on the fair and appropriate use of information Goal to ensure data transferred to non-European countries is protected Based on set of seven principles for data privacy Concern that U.S. government can invoke USA PATRIOT Act to access data.

توجيه الاتحاد الأوروبي لحماية البيانات. يتطلب من الشركات التي تمارس الأعمال التجارية داخل حدود 15 دولة أوروبية تنفيذ مجموعة من توجيهات الخصوصية بشأن الاستخدام العادل والمناسب للمعلومات الهدف لضمان حماية البيانات المنقولة إلى دول غير أوروبية استنادًا إلى مجموعة من سبعة مبادئ لخصوصية البيانات مخاوف الولايات المتحدة. يمكن للحكومة استدعاء USA PATRIOT Actللوصول إلى البيانات.

BBB Online and TRUST Independent initiatives that favor an industry-regulated approach to data privacy bBBBOnLine reliability seal or a TRUSTe data privacy seal demonstrates that Web site adheres to high level of data privacy Seals Increase consumer confidence in site Help users make more informed decisions about whether to release personal information.

مبادرات BBB Onlineو TRUSTالمستقلة التي تفضل اتباع نهج منظم في الصناعة لخصوصية البيانات يوضح ختم موثوقية bBBBOnLineأو ختم خصوصية بيانات TRUSTeأن موقع الويب يلتزم بمستوى عالٍ من خصوصية البيانات. للإفصاح عن المعلومات الشخصية.

Access to government records الوصول إلى السجلات الحكومية

Freedom of Information Act (1966 amended 1974) Grants citizens the right to access certain information and records of the federal government upon request Exemptions bar disclosure of information that could: Compromise national security Interfere with active law enforcement investigation Invade someone's privacy

قانون حرية المعلومات (1966 المُعدّل في 1974) يمنح المواطنين الحق في الوصول إلى معلومات وسجلات معينة للحكومة الفيدرالية عند الطلب.
استثناءات حظر الإفصاح عن المعلومات التي يمكن أن: تتعارض مع الأمن القومي وتتعارض مع تحقيق إنفاذ القانون النشط وتنتهك خصوصية شخص ما

The Privacy Act of 1974 Prohibits government agencies from concealing the existence of any personal data record-keeping system Outlines 12 requirements that each record-keeping agency must meet CIA and law enforcement agencies are excluded from this act Does not cover actions of private industry.

يحظر قانون الخصوصية لعام 1974 على الوكالات الحكومية إخفاء وجود أي نظام لحفظ سجلات البيانات الشخصية. يحدد 12 من المتطلبات التي يجب أن تفي بها كل وكالة حفظ سجلات وكالة المخابرات المركزية ووكالات إنفاذ القانون مستثناة من هذا القانون لا يغطي إجراءات الصناعة الخاصة.

الفصل الرابع

من سلسلة محاضرات لمساق

أخلاقيات المهنة في تكنولوجيا المعلومات

د. محمد فوزي العقاد

Key Privacy and Anonymity Issues قضايا الخصوصية وإخفاء الهوية الرئيسية

- Identity theft
- Electronic discovery
- Consumer profiling
- Treating customer data responsibly
- Workplace monitoring
- Advanced surveillance technology.
- Identity Theft Theft of key pieces of personal information to impersonate a person, including: Name Address Date of birth Social Security number Passport number Driver’s license number Mother’s maiden name.
- Fastest-growing form of fraud in the United States Consumers and organizations are becoming more vigilant and proactive in fighting identity theft Four approaches used by identity thieves Create a data breach Purchase personal data Use phishing to entice users to give up data Install spyware to capture keystrokes of victims.

سرقة الهوية

الاكتشاف الإلكتروني

تنميط المستهلك

التعامل مع بيانات العميل بمسؤولية

مراقبة مكان العمل

تكنولوجيا المراقبة المتقدمة.

سرقة الهوية تعني سرقة أجزاء أساسية من المعلومات الشخصية لانتحال شخصية شخص ، بما في ذلك: الاسم العنوان تاريخ الميلاد رقم الضمان الاجتماعي رقم جواز السفر رقم رخصة القيادة اسم الأم قبل الزواج.

كما ان أسرع أشكال الاحتيال نموًا في الولايات المتحدة أصبح المستهلكون, واصبحت المؤسسات أكثر يقظة واستباقية في مكافحة سرقة بيانات المستخدمين , هناك أربعة أساليب يستخدمها لصوص الهوية مثل إنشاء اختراقات للبيانات و شراء البيانات الشخصية واستخدم التصيد الاحتيالي لإغراء المستخدمين بالتخلي عن بياناتهم الخاصة عن طريق تثبيت برنامج تجسس لالتقاط البيانات التي يقوم الضحايا بكتابتها على حواسيبهم.

Identity Theft (cont'd.) سرقة الهوية

Data breaches of large databases To gain personal identity information May be caused by: Hackers Failure to follow proper security procedures Purchase of personal data Black market for: Credit card numbers in bulk—$.40 each Logon name and PIN for bank account—$10Identity information—including DOB, address, SSN, and telephone number—$1 to $15.

Phishing Stealing personal identity data by tricking users into entering information on a counterfeit Web site Spyware Keystroke-logging software Enables the capture of: Account usernames Passwords Credit card numbers Other sensitive information Operates even if infected computer is not online.
Identity Theft and Assumption Deterrence Act of 1998 was passed to fight fraud Identity Theft Monitoring Services Monitor the three major credit reporting agencies (TransUnion, Equifax, and Experian)Monitor additional databases (financial institutions, utilities, and DMV).

يتم اختراق قواعد البيانات عن طريق تزييف هوية المستخدم وذلك عن طريق الهاكرز , او عدم القدرة على اتباع سياسة حماية فعالة, بيع البيانات الخاصة, السوق السوداء لبيع بطاقات الائتمان بالجملة مقابل 0.40 سنتا للرقم تشمل بيانات تسجيل الدخول وتاريخ الميلاد والعنوان و ارقام التامين الاجتماعي , كما يعتبر التصيد وسيلة لسرقة البيانات الخاصة عن طريق خداع المستخدمين لإدخال بياناتهم في مواقع غير آمنة وذلك بهدف سرقة حسابات المستخدمين وكلمات المرور وبطاقات الدفع المسبق وبيانات اخرى حساسة ومهمة. تعتبر المادة سنة 1998 رادعا لسرقة الهوية بهدف مكافحة سرقة بيانات المستخدمين, تقوم خدمات مراقبة السرقة بمراقبة الوكالات الثلاث الرئيسية ترانس يونيون, اكويفاكس و اكسبيريان ومراقبة قواعد بيانات اخرى تشمل مراكز ماليه و مراكز خدمات و مركز خدمات السيارات DVM department of motor vehicles

Electronic Discovery الاكتشاف الإلكتروني

Collection, preparation, review, and production of electronically stored information for use in criminal and civil actions Quite likely that information of a private or personal nature will be disclosed during e-discovery Federal Rules of Procedure define e-discovery processes

جمع المعلومات المخزنة إلكترونيًا وإعدادها ومراجعتها وإنتاجها لاستخدامها في الإجراءات الجنائية والمدنية من المحتمل جدًا أن يتم الكشف عن المعلومات ذات الطبيعة الخاصة أو الشخصية أثناء الاكتشاف الإلكتروني. تحدد القواعد الإجرائية الفيدرالية عمليات الاكتشاف الإلكتروني

Raises many ethical issues Should an organization attempt to destroy or conceal incriminating evidence? To what degree must an organization be proactive and thorough in providing evidence? Should an organization attempt to “bury” incriminating evidence in a mountain of trivial, routine data?

يثير العديد من القضايا الأخلاقية هل يجب على المنظمة أن تحاول تدمير أو إخفاء أدلة الإدانة؟ إلى أي درجة يجب أن تكون المنظمة استباقية وشاملة في تقديم الأدلة؟ هل ينبغي لمنظمة ما أن تحاول "دفن" أدلة الإدانة في جبل من البيانات الروتينية التافهة

Consumer Profiling (cont’d.) تنميط المستهلك

Companies openly collect personal information about Internet users Cookies Text files that a Web site can download to visitors’ hard drives so that it can identify visitors later Tracking software analyzes browsing habits Similar controversial methods are used outside the Web environment.

تجمع الشركات علنًا معلومات شخصية عن مستخدمي الإنترنت ملفات تعريف الارتباط ملفات نصية يمكن لموقع ويب تنزيلها على محركات الأقراص الثابتة للزوار حتى يتمكن من التعرف على الزائرين لاحقًا. برامج التتبع تحلل عادات التصفح تُستخدم طرق مماثلة مثيرة للجدل خارج بيئة الويب.

Aggregating consumer data Databases contain a huge amount of consumer behavioral data Affiliated Web sites are served by a single advertising network Collecting data from

تجميع قواعد بيانات المستهلك تحتوي على قدر هائل من البيانات السلوكية للمستهلكين يتم تقديم مواقع الويب التابعة من خلال شبكة إعلانية واحدة تجمع البيانات منها..

Four ways to limit or stop the deposit of cookies on hard drives Set the browser to limit or stop cookies Manually delete them from the hard drive Download and install a cookie-management program Use anonymous browsing programs that don’t accept cookies.

أربع طرق للحد من إيداع ملفات تعريف الارتباط على محركات الأقراص الثابتة أو إيقافه اضبط المتصفح على تقييد ملفات تعريف الارتباط أو إيقافها ، احذفها يدويًا من محرك الأقراص الثابتة. تنزيل برنامج إدارة ملفات تعريف الارتباط وتثبيته ، استخدم برامج تصفح مجهولة لا تقبل ملفات تعريف الارتباط.

Personalization software Used by marketers to optimize the number, frequency, and mixture of their ad placements Rules-based Collaborative filtering Demographic filtering Contextual commerce Consumer data privacy Platform for Privacy Preferences (P3P)Shields users from sites that don’t provide the level of privacy protection desired

برنامج التخصيص الذي يستخدمه المسوقون لتحسين عدد مواضع إعلاناتهم وتكرارها ومزيجها. المطلوب الحماية.

.

Treating Consumer Data Responsibly معالجة بيانات المستهلك بمسؤولية

Strong measures are required to avoid customer relationship problems Companies should adopt: Fair Information Practices1980 OECD privacy guidelines. Federal Trade Commission responsible for protecting privacy of U.S. consumers Chief privacy officer (CPO)Executive to oversee data privacy policies and initiatives

مطلوب تدابير قوية لتجنب مشاكل العلاقة مع العملاء يجب على الشركات تبني: ممارسات المعلومات العادلة 1980 إرشادات الخصوصية لمنظمة التعاون الاقتصادي والتنمية. لجنة التجارة الفيدرالية المسؤولة عن حماية خصوصية المستهلكين الأمريكيين الرئيس التنفيذي للخصوصية ((CPOللإشراف على سياسات ومبادرات خصوصية البيانات

Workplace Monitoring Employers monitor workers
مراقبة مكان العمل حيث يقوم أرباب العمل بمراقبة العمال

Protect against employee abuses that reduce worker productivity or expose employer to harassment lawsuits Fourth Amendment cannot be used to limit how a private employer treats its employees Public-sector employees have far greater privacy rights than in the private industry Privacy advocates want federal legislation. To keep employers from infringing upon privacy rights of employees.

الحماية من انتهاكات الموظفين التي تقلل من إنتاجية العمال أو تعرض صاحب العمل لقضايا مضايقة لا يمكن استخدام التعديل الرابع للحد من كيفية تعامل صاحب العمل الخاص مع موظفيه يتمتع موظفو القطاع العام بحقوق خصوصية أكبر بكثير مما هي عليه في الصناعة الخاصة. لمنع أصحاب العمل من التعدي على حقوق الخصوصية للموظفين.

Advanced Surveillance Technology تقنية المراقبة المتقدمة

Camera surveillance Many cities plan to expand surveillance systems. Advocates argue people have no expectation of privacy in a public place Critics concerned about potential for abuse Global positioning system (GPS) chips Placed in many devices Precisely locate users Banks, retailers, airlines eager to launch new services based on knowledge of consumer location.

لمراقبة بالكاميرات:: تخطط العديد من المدن لتوسيع أنظمة المراقبة. يجادل المدافعون بأن الناس لا يتوقعون الخصوصية في مكان عام النقاد قلقون من احتمال إساءة استخدام رقائق نظام تحديد المواقع العالمي (GPS) الموضوعة في العديد من الأجهزة تحديد مواقع المستخدمين بدقة البنوك وتجار التجزئة وشركات الطيران المتلهفة لإطلاق خدمات جديدة بناءً على معرفة موقع المستهلك.

Summary

- The right of privacy is “the right to be left alone—the most comprehensive of rights, and the right most valued by a free people.”
- Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one’s personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).
- The use of information technology in business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used. A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales.
- The Fourth Amendment reads, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” The courts have ruled that without a reasonable expectation of privacy, there is no privacy right to protect.
- Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. For many, the existing hodgepodge of privacy laws and practices fails to provide adequate p

- الحق في الخصوصية هو "الحق في أن تُترك وشأنه - أكثر الحقوق شمولاً ، والحق الذي يحترمه الأشخاص الأحرار".
- خصوصية المعلومات هي مزيج من خصوصية الاتصالات (القدرة على التواصل مع الآخرين دون مراقبة هذه الاتصالات من قبل أشخاص أو منظمات أخرى) وخصوصية البيانات (القدرة على تقييد الوصول إلى البيانات الشخصية للفرد من قبل الأفراد والمؤسسات الأخرى من أجل ممارسة مهمة كبيرة. درجة التحكم في تلك البيانات واستخدامها).
- يتطلب استخدام تكنولوجيا المعلومات في الأعمال التجارية موازنة احتياجات أولئك الذين يستخدمون المعلومات التي يتم جمعها مقابل حقوق ورغبات الأشخاص الذين يتم استخدام معلوماتهم. هناك حاجة إلى مجموعة من الأساليب - القوانين الجديدة والحلول التقنية وسياسات الخصوصية - لموازنة المقاييس.
- ينص التعديل الرابع على ما يلي: "لا يجوز انتهاك حق الأشخاص في أن يكونوا آمنين في أشخاصهم ومنازلهم وأوراقهم وآثارهم ، ضد عمليات التفتيش والمصادرة غير المعقولة ، ولن يتم إصدار أية أوامر قضائية ، ولكن بناءً على سبب محتمل ، بدعم من القسم أو تأكيد ، ولا سيما وصف المكان الذي سيتم تفتيشه والأشخاص أو الأشياء التي سيتم الاستيلاء عليها ". قضت المحاكم بأنه بدون توقع معقول للخصوصية ، لا يوجد حق حماية للخصوصية.
- اليوم ، بالإضافة إلى الحماية من التدخل الحكومي ، يريد الناس ويحتاجون إلى حماية الخصوصية من الصناعة الخاصة. بالنسبة للكثيرين ، فشل الخليط الحالي من قوانين وممارسات الخصوصية في توفير p