專 題 企 劃

授權使用公司內部電腦之範圍—United States v. David Nosal判決之導讀（含法學英文）

前臺灣臺北地方法院檢察署檢察官、現美國加州執業律師 陳仕蘭

電腦成為每人每天生活中不可或缺的一部分，但是電腦也改變了人類的生活習慣，電腦之使用與資料儲存使得不論是公部門或者是私部門對於內部機密文件的管理以及保密變得相對困難且易於遭到拷貝或竊取，然而傳統竊盜或是背信之定義，對於易於拷貝或者另行儲存之電腦資料，在適用於刑事法律時，傳統的構成要件定義，也因為電腦的介入而受到挑戰，因此不論是公部門或者是私人公司都制定有內部電腦使用政策，而每當消費者使用Google或是Facebook的電子郵件信箱或者是登錄新的帳戶時，消費者都需要同意服務提供者制定之使用規則（Terms of service or terms of agreement）才可繼續帳號之登錄或是電子信箱之使用，一旦員工或者是使用者違反電腦使用規則而取得資料時，是否因此而有刑事責任？

美國聯邦法院針對此議題並無定論，United States v. David Nosal為聯邦第九上訴巡迴法院針對此一法律問題所作出之判決。

案件事實簡介

David Nosal為執行搜尋公司Korn/Kerry之前員工，於其離職後，他說服尚在Korn/Kerry工作之同事幫助他建立另一間搜尋公司，而Korn/Kerry之員工利用自己之帳號密碼登入公司之電腦並且進入公司之保密資料庫內下載客戶名單以及聯絡資訊，並將此保密資訊轉交給David Nosal.

該公司員工經公司授權可以自己之帳號密碼登入公司之電腦並下載資訊，但是該公司之政策禁止員工將所下載之應秘密資訊做不當揭露，聯邦檢察官據此起訴David Nosal 20項罪名，其中包括Computer Fraud And Abuse Act (CFAA) 18 U.S.C 1030(a)(4)之意圖詐欺

超出授權範圍侵入受保護之電腦並因此取得有價值之物（原文：Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value.）

本案爭點：

David Nosal請求聯邦上訴法院撤銷檢方對於CFAA 18 U.S.C 1030(a)(4)之控訴，並答辯稱：CFAA乃針對駭客所做之刑事處罰，並非對於經授權進入電腦後對取得資料做不當使用所做之處罰，聯邦第九巡迴法院應遵循其於前案LVRC Holdings LLC v. Brekka中針對18 U.S.C.§1030[1]之法條文字對於未經授權以及超過授權範圍做限縮性之解釋，因此不應將公司之內部政策作為授權範圍之界定

判決摘要：

多數意見認為所謂的授權範圍應做限縮性解釋，一但使用有效之帳號密碼登入公司電腦後，即便將取得之公司內部機密資料做不當之使用，亦不能以刑事法律處罰，否則會導致刑事處罰範圍過大且不明確，且會導致將無害但有違反公司內部制定使用電腦政策之瑣碎行為（使用公司電腦查天氣或是線上購物）列入刑罰之懲罰中

以下為多數意見判決摘要：

The CFAA defines “exceeds authorized access” as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not

1 18 U.S.C.§ 1030 –
(a) Whoever –
(2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –
(A) Information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) Information from any department or agency of the United States; or
(C) Information from any protected computer;
(4) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This language can be read either of two ways: First, as Nosal suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but

accesses customer data: He would "exceed authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to

someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be

authorized to access customer lists in order to do his job but not to send them to a competitor.

In the case of the CFAA, the broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet without any culpable intent. Were we to adopt the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct. Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes.

法學英文

Access—侵入，進入
Authorization—授權
Exceed—超過，超出
Colloquial—口語的，非正式的
Physical—實體
Culpable—值得譴責的, 有罪責的
Interpretation—解釋，詮釋
Procrastinate—拖延，遲疑

Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching TV on your work computer, you could be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement. Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law. Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read. Consider the typical corporate policy that computers can be used only for business purposes. What exactly is a "nonbusiness purpose"? If you use the computer to check the weather report for a business trip? For the company softball game? For your vacation to Hawaii? And if minor personal uses are tolerated, how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?

Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the New York Times to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.

法學英文

Federal crimes—美國刑事管轄權區分為州刑法與聯邦刑法，兩者屬不同管轄權，基本上若是刑事犯罪屬於跨越州際之犯罪，應由聯邦司法體系具有司法管轄權，由聯邦檢察官起訴，並由聯邦法院審理，網際網路屬跨州犯罪，管轄權均屬聯邦司法體系

Dalliance—不正經的，不認真的

Prosecute—起訴

Ubiquitous—廣泛的，常見的

Arbitrary—恣意，沒有理由的
Torts—類似我國之侵權行為法
Manipulate—操弄，操控
Criminal liability—刑事責任
Vagary—無法預見的，未知的
Opaque—不透明的，難以理解的
Innocuous—無害的
Sudoku—數字遊戲

The effect this broad construction of the CFAA has on workplace conduct pales by comparison with its effect on everyone else who uses a computer, smart-phone, iPad, Kindle, Nook, X-box, Blu–Ray player or any other Internet-enabled device. The Internet is a means for communicating via computers: Whenever we

access a web page, commence a download, post a message on somebody's Facebook wall, shop on Amazon, bid on eBay, publish a blog, rate a movie on IMDb, read www.NYT.com, watch YouTube and do the thousands of other things we routinely do online, we are using one computer to send commands to other computers at remote locations. Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands. For example, it's not widely known that, up until very recently, Google forbade minors from using its services. See Google Terms of Service, effective April 16, 2007—March 1, 2012, § 2.3, http://www.google. com/intl/en/policies/terms/archive/20070416 ("You may not use the Services and may not accept the Terms if ... you are not of legal age to form a binding contract with Google...."). Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents—and their parents and teachers into delinquency contributors. Similarly, Facebook makes it a violation of the terms of service to let anyone log into your account. See Facebook Statement of Rights and Responsibilities § 4.8 http://www.facebook.com/legal/terms ("You will not share your password, ... let anyone else access your account, or do anything else that might jeopardize the security of your account.") . Yet it's very common for people to let close friends and relatives check their email or access their online accounts. Some may be aware that, if discovered, they may suffer a rebuke from the ISP or a loss of access,

but few imagine they might be marched off to federal prison for doing so.

Or consider the numerous dating websites whose terms of use prohibit inaccurate or misleading information. See, e.g., eHarmony Terms of Service § 2(I),

http://www.eharmony.com/about/terms ("You will not provide inaccurate, misleading or false information to eHarmony or to any other user.") Or eBay and Craigslist, where it's a violation of the terms of use to post items in an inappropriate category.

See, e.g., eBay User Agreement, http://pages.ebay.com/help/policies/user-agreement.html ("While using eBay sites, services and tools, you will not: post content or items in an inappropriate category or areas on our sites and services ....")

Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy, or describing yourself as "tall, dark and

handsome," when you're actually short and homely, will earn you a handsome orange jumpsuit.

法學英文

Pale—包括
Dimly—微弱，細微
Juvenile Delinquents—少年非行，少年違法行為
Delinquency contributors—促成違反行為之人
Jeopardize—置於危險狀態
Rebuke—警告

Not only are the terms of service vague and generally unknown—unless you look real hard at the small print at the bottom of a webpage—but website owners retain the right to change the terms at any time and without notice. See, e.g., YouTube Terms of Service § 1.B, http://www.youtube.com/t/terms ("YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions.") Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever. The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't

have to live at the mercy of our local prosecutor. Cf. United States v. Stevens, 559 U.S. 460, 130 S.Ct. 1577, 1591, 176 L.Ed.2d 435 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly."). And it's not clear we can trust the government when a tempting target comes along. Take the case of the mom who posed as a 17–year–old boy and cyber-bullied her daughter's classmate. The Justice Department prosecuted her under 18 U.S.C. § 1030(a)(2)(C) for violating MySpace's terms of service, which prohibited lying about identifying information, including age. See United States v. Drew, 259 F.R.D. 449 (C.D.Cal.2009). Lying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight. The difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after. In United States v. Kozminski, 487 U.S. 931, 108 S.Ct. 2751, 101 L.Ed.2d 788 (1988), the Supreme Court refused to adopt the government's broad interpretation of a statute because it would "criminalize a broad range of day-to-day activity." Id. at 949, 108 S.Ct. at 2763. Applying the rule of lenity, the Court warned that the broader statutory interpretation would "delegate to prosecutors and juries the inherently legislative task of determining what type of ... activities are so morally reprehensible that they should be punished as crimes" and would "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction." By giving that much power to prosecutors, we're inviting discriminatory and arbitrary enforcement.

法學英文

Discretion—裁量
Revise—修正
Be bound by—受拘束
At the mercy of—憐憫
Uphold—維持，支持
Cyber-bullied—網路霸凌
Puffery—誇大
Rule of lenity—寬容，寬鬆
Delegate—授與權力

反對意見：

反對意見則認為，多數意見之擔憂屬杞人憂天，反對意見認為，從本條項之字面即可清楚認定被告從使用帳號密碼登入公司電腦時，即已具有將取得之電腦資料做不當使用之詐欺犯意，多數意見擔憂擴張解釋會將無害之違反公司內部使用政策之行為，變成違反刑事法之行為亦屬多慮，多數意見所舉例之無害行為，本就與本條項之文字無關，本案被告之行為應已違反CFAA 18 U.S.C 1030(a)(4) 之意圖詐欺，超出授權範圍侵入受保護之電腦，並因此取得有價值之物。

反對意見之摘要：

This case has nothing to do with playing sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values. It has everything to do with stealing an employer's valuable information to set up a competing business with the purloined data, siphoned away from the victim, knowing such access and use were prohibited in the defendants' employment contracts. The indictment here charged that Nosal and his co-conspirators knowingly exceeded the access to a protected company computer they were given by an executive search firm that employed them; that they did so with the intent to defraud; and further, that they stole the victim's valuable proprietary information by means of that fraudulent conduct in order to profit from using it. In ridiculing scenarios not remotely presented by this case, the majority does a good job of knocking down straw men — far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy. The majority also takes a plainly written statute and parses it in a hyper-complicated way that distorts the obvious intent of Congress. No other circuit that has considered this statute finds the problems that the majority does. 18 U.S.C. § 1030(a)(4) is quite clear. It states, in relevant part: (a) Whoever— (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . shall be punished . . . . Thus, it is perfectly clear that a person with both the requisite mens rea and the specific intent to defraud — but only such persons — can violate this subsection in one of two ways: first, by accessing a computer without authorization, or second, by exceeding authorized

access. 18 U.S.C. § 1030(e)(6) defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." "As this definition makes clear, an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.' " LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)

法學英文

Purloin—竊取
Siphoned away—非法取得
Indictment—起訴，通常指經過大陪審團（grand jury）決定起訴之案件
Charge—控訴
Defraud—詐欺取財
Proprietary—擁有所有權
Fraudulent—詐欺的
Parse—劃分成小部分的
Distort—扭曲

Mens rea—指特定刑事犯罪需具備之主觀犯意，刑事犯罪需同時具備mens rea以及actus reus（有意識之客觀行為）始得成罪，每種刑事犯罪要求之主觀犯意不盡相同, 本案所涉及之犯罪為一特定犯意犯罪（specific intent crime），行為人不僅須意識到自身所做之行為為非法並且了解行為所造成之後果Be entitled to—對…擁有權利，通常指需有法律依據或者有契約上之依據, 僅僅主觀之期待並非權利

"The definition of the term 'exceeds authorized access' from § 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer. The plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer." Id. at 1135. In Brekka, we explained that a person "exceeds authorized access" when that person has permission to access a computer but accesses information on the computer that the person is not entitled to access at 1133. In that case, an employee allegedly emailed an employer's

proprietary documents to his personal computer to use in a competing business at 1134. We held that one does not exceed authorized access simply by "breach[ing] a state law duty of loyalty to an employer" and that, because the employee did not breach a contract with his employer, he could not be liable under the Computer Fraud and Abuse Act. Id. at 1135, 1135 n.7. This is not an esoteric concept. A bank teller is entitled to access a bank's money for legitimate banking purposes, but not to take the bank's money for himself. A new car buyer may be entitled to take a vehicle around the block on a test drive. But the buyer would not be entitled — he would "exceed his authority" — to take the vehicle to Mexico on a drug run. A person of ordinary intelligence understands that he may be totally prohibited from doing something altogether, or authorized to do something but prohibited from going beyond what is authorized. This is no doubt why the statute covers not only "unauthorized access," but also "exceed[ing] authorized access." The statute contemplates both means of committing the theft. The majority holds that a person "exceeds authorized access" only when that person has permission to access a computer generally, but is completely prohibited from accessing a different portion of the computer (or different information on the computer). The majority's interpretation conflicts with the plain language of the statute. Furthermore, none of the circuits that have analyzed the meaning of "exceeds authorized access" as used in the Computer Fraud and Abuse Act read the statute the way the majority does. Both the Fifth and Eleventh Circuits have explicitly held that employee who knowingly violate clear company computer restrictions agreements "exceed authorized access" under the CFAA.

Breach—違反，侵犯

Esoteric—專精的，專業的

Contemplate—包含

In United States v. John, 597 F.3d 263, 271-73 (5th Cir. 2010), the Fifth Circuit held that an employee of Citigroup exceeded her authorized access in violation of § 1030(a)(2) when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud. As the Fifth Circuit noted in John, "an employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business. An employee would 'exceed authorized access' if he or she used that access to obtain or steal information as part

of a criminal scheme." Id. at 271 (alteration in original). At the very least, when an employee "knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of [a criminally fraudulent] scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access.' " Id. at 273. Similarly, the Eleventh Circuit held in United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), that an employee of the Social Security Administration exceeded his authorized access under § 1030(a)(2) when he obtained personal information about former girlfriends and potential paramours and used that information to send the women flowers or to show up at their homes. The court rejected Rodriguez's argument that unlike the defendant in John, his use was "not criminal." The court held: "The problem with Rodriguez's argument is that his use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access." Id.; see also EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583-84 (1st Cir. 2001) (holding that an employee likely exceeded his authorized access when he used that access to disclose information in violation of a confidentiality agreement). The Third Circuit has also implicitly adopted the Fifth and Eleventh circuit's reasoning. In United States v. Teague, 646 F.3d 1119, 1121-22 (8th Cir. 2011), the court upheld a conviction under § 1030(a)(2) and (c)(2)(A) where an employee of a government contractor used his privileged access to a government database to obtain President Obama's private student loan records.

Conviction—有罪判決，acquittal為無罪判決

The indictment here alleges that Nosal and his coconspirators knowingly exceeded the authority that they had to access their employer's computer, and that they did so with the intent to defraud and to steal trade secrets and proprietary information from the company's database for Nosal's competing business. It is alleged that at the time the employee coconspirators

accessed the database they knew they only were allowed to use the database for a legitimate business purpose because the co-conspirators allegedly signed an agreement which restricted the use and disclosure of information on the

database except for legitimate Korn/Ferry business. Moreover, it is alleged that before using a unique username and password to log on to the Korn/Ferry computer and database, the employees were notified that the information stored on those computers were the property

of Korn/Ferry and that to access the information without relevant authority could lead to disciplinary action and criminal prosecution. Therefore, it is alleged, that when Nosal's co-conspirators accessed the database to obtain Korn/Ferry's secret source lists, names, and

contact information with the intent to defraud Korn/Ferry by setting up a competing company to take business away using the stolen data, they "exceed[ed their] authorized access" to a computer with an intent to defraud Korn/Ferry and therefore violated 18 U.S.C. § 1030(a)(4). If true, these allegations adequately state a crime under a commonsense reading of this particular subsection. Furthermore, it does not advance the ball to consider, as the majority does, the parade of horribles that might occur under different subsections of the CFAA, such as subsection UNITED STATES v. NOSAL 3877 (a)(2)(C), which does not have the scienter or specific intent to defraud requirements that subsection (a)(4) has. Maldonado v. Morales, 556 F.3d 1037, 1044 (9th Cir. 2009) ("The role

of the courts is neither to issue advisory opinions nor to declare rights in hypothetical cases, but to adjudicate live cases or controversies.") Other sections of the CFAA may or may not be unconstitutionally vague or pose other problems. We need to wait for an actual case or controversy to frame these issues,

rather than posit a laundry list of wacky hypotheticals. I express no opinion on the validity or application of other subsections of 18 U.S.C § 1030, other than § 1030(a)(4), and with all due respect, neither should the majority.

The majority's opinion is driven out of a well meaning but ultimately misguided concern that if employment agreements or internet terms of service violations could subject someone to criminal liability, all internet users will suddenly become criminals overnight. I fail to see how anyone can seriously conclude that reading ESPN.com in contravention of office policy could come within the ambit of 18 U.S.C. § 1030(a)(4), a statute explicitly requiring an intent to defraud, the obtaining of something of value by means of that fraud, while doing so "knowingly." And even if an imaginative judge can conjure up far-fetched hypotheticals producing federal prison terms for accessing word puzzles, jokes, and sports scores while at work, well, . . . that is what an as-applied challenge

is for. Meantime, back to this case, 18 U.S.C. § 1030(a)(4) clearly is aimed at, and limited to, knowing and intentional fraud. Because the indictment adequately states the elements of a valid crime, the district court erred in dismissing the charges. I respectfully dissent.

Coconspirators—共犯
Allegation—指控
Scienter—主觀犯意
Adjudicate—司法裁決
In contravention of—違反
Within the ambit of—within the scope of—範圍內

小結：

本案針對18 U.S.C 1030(a)(4)授權範圍之解釋，在各個聯邦上訴巡迴法院[2]意見不並不一致，許多其他聯邦上訴法院亦採用反對意見之見解，事實上多數意見亦承認僅從法條文字上確實可做較為擴張之解釋，而各個聯邦上訴法院本身之意見不受彼此約束，因此國會業已著手針對此法條做修正。

2 美國共有13個聯邦上訴巡迴法院，其中第九聯邦上訴巡迴法院管轄範圍為13個聯邦上訴法院中管轄範圍最為廣大，包含加州，華盛頓州，亞利桑納州，內華達，愛達荷，奧勒岡，蒙大拿，阿拉斯加州以及夏威夷州等https://en.wikipedia.org/wiki/United_States_Court_of_Appeals_for_the_Ninth_Circuit