探討如何避免自己被網上起底

講者：　香港高登討論區行政總裁、網上服務供應商聯盟主席、iProA 常務理事林祖舜先生

講座日期：2011 年 6 月 11 日

免責聲明：以下講座內容僅代表講者意見，並不反映個人資料私隱專員公署及其他合辦機構的立場)

引言

大家知道何謂「網上起底」嗎？網絡世界是個虛擬世界，但即使你使用虛擬姓名，仍然可能讓人知道你在現實世界的身份。為甚麼？這是我們今天探討的議題，內容有以下數點：

- ✧ 起底的目的：網民的真正身份本應不為人知，其個人資料包括真實姓名、地址、電話等等，卻可能突然變得人所共知。公開這些資料的人，動機何在？很多知道我是高登網主的人都會向我說：我很害怕，害怕一上網便被起底！今天，我們會探討被起底的原因，看看你有沒有機會成為下一個被起底的目標。

- ✧ 起底的常見方法：在網上世界本應不為人知的現實身份，究竟如何被發現？起底者用的是甚麼方法？

- ✧ 網絡密碼安全小提示：我們身處網絡世界，應該像在現實世界一樣，事事小心，可能還要加倍小心。要如何保護自己的資料，才能防止被起底？我們在各個網站享用各種服務時，可能會被要求設置密碼，而我會提醒大家設置安全密碼的方法。一些駭客襲擊網站後，取得了不少用戶的密碼並加以分析，發現一些很多人使用的「常用密碼」。如果你也是這些「常用密碼」的使用者，就要小心了。

- ✧ 如何保障個人資料避免被網上被底：提供一些小貼士教你如何避免被網上起底。

起底的目的

如果大家留意報章雜誌，也會得知一些起底個案。不過，報章雜誌經常一概而論，

視起底為「網絡欺凌」。其實，「網絡欺凌」只是起底目的之一，決非唯一目的，兩者之間不可劃上等號。起底有多種目的，以下我們會逐一探討。

第一個原因是**網絡罵戰（flaming）**，是網絡最常見的非抑制行為。網絡罵戰，無非是在網上吵架，可能會發展至言語過激，刻薄至人身攻擊的地步。不過，即使言語再激烈，大部分罵戰者都不會有「把對方從現實世界揪出來」的念頭，通常只是就議題進行言語攻擊。如果發展至起底，可能是因為想知道當事人的資料，例如職業、在哪所學校讀書等，但始終沒有把對方揪出來的念頭。

說些例子。遼寧女子咒罵四川地震受害人[1]，還有奧地利獸父案[2]，都是激起公憤的事件，引發網民口誅筆伐。部分網民言辭激進，不過沒有欺凌當事人的意圖，也無意把他們從現實中揪出來。在這些情況中，「起底」的目的，不過是為了在網上怒罵當事人。

第二個原因就真的是**網絡欺凌**。很多媒體都使用過這字眼，但未必使用得準確。「網絡欺凌」所指的，通常是兒童或青少年透過互聯網、手機等網絡傳播技術，傳播文字、圖片等，以折磨、騷擾、威逼、羞辱另一兒童或青少年。欺凌是兒童和青少年之間的行為，而利用網絡傳播技術進行的，就是網絡欺凌。如果成年人透過網絡傳播技術，傳播文字、圖片以威逼、羞辱另一成年人，則稱為「網絡侵擾」。某著名反網絡欺凌網站的主頁，也明確指出網絡欺凌只會發生在未成年人士之間。

明白了「網絡欺凌」的意思，我們就知道起底的另一目的：兒童或青少年打算羞辱、威嚇、傷害另一兒童或青少年，故此對目標進行起底，希望得到更多個人資料以折磨對方。

第三個原因，就是剛才提及的、發生在成年人之間的**網絡侵擾**。例如北京奧運火炬接力於海外進行時，一名來自青島的在美留學生被發現高舉藏獨旗幟。網民群起攻之，甚至發動「人肉搜尋」，找出這人的底細。最後，這名學生的資料，例如她在青島的住址、電話等，全部被公開了。

不過，這次事件在網民發洩情緒後仍未完結。這次起底的目的，真的是要在現實世界上騷擾當事人。留學生被起底後，很多網民在其家門前聚集抗議，可見網上起底有機會波及現實世界。

---

[1] 2008 年 5 月 21 日，即 512 地震後一周左右，網上出現一段遼寧女子咒罵地震災民數分鐘之久的短片。

[2] 2009 年，奧地利發現一名父親禁錮強暴女兒二十四年之久，並誕下七名子女。

這件事非常轟動，有人把網民的激進舉動形容為「網絡群體性事件」，即是有人在網上發起行動，並在現實世界執行。由於不是兒童或青少年所幹的，所以不應稱為「網絡欺凌」，不過時下不少媒體經常錯用這字眼。

第四個起底的原因，就是**網絡公審**。網民自稱起底並非無的放矢，不是為了發洩罵人或騷擾別人，而是調查壞人的底細。當然，何謂「壞人」，本來就有商榷餘地，難以一概而論，因為每人的道德標準都不一樣。不過，部分網民事先已認定某人為壞人，為了「公審」而找出這人的底細，再決定怎樣「處罰」這「壞人」。

以上說了不少起底目的，當中「網絡欺凌」肯定是不正確的，因為所有兒童和青少年都應該受保護。不過，其餘三個目的（罵戰、侵擾、公審）是否合理，則帶有較濃重的主觀成分。例如在網上被公審的是否壞人？這些事很難一概評論，也不屬於今天的討論範圍。

不過，在起底行動中「借刀」則肯定不對。所謂「借刀」，就是「借刀殺人」，在網上頗為普遍。網上消息的特點，就是「真亦假時假亦真」，好些看起來簡直像新聞報導的網上消息，原來是虛構的。然而，即使是假新聞，也可以透過網絡極速傳播，傳到所有人耳中。因此，某些人會在網上散播假新聞，陷害他們的敵人。

借刀者知道網民喜歡公審壞人，所以誣蔑其敵人為壞人，又或者在網民對另一壞人起底時，突然指出其敵人與該壞人有點相似（例如身高差不多，或者唸同一所學校），謊稱其敵人就是該壞人。這就是「借刀」，為達到個人目的而欺騙網民，明顯是不正確的行為。

起底的常見方法

各位了解起底目的後，如果肯定自己沒可能成為被起底的人，當然可以安心遨遊網際了。然而，有可能成為起底目標，也不等於可能被起底——像我這樣的主講者，全名和工作早已向外公開，自然容易起底，但一般人的資料又怎會人盡皆知？所以要起底也有難度。

常見的起底途徑，包括搜尋器、社交網絡、朋友於討論區「出賣」被起底者的資料、駭客軟件、檔案分享軟件、不誠實的電腦維修員……這些都是網民曾經使用的起底方法，我們會逐一探討。

起底的第一步，必定是使用**搜尋器**，因為搜尋器已經越來越強大。十年前，要用搜尋器找出某人資料是很困難的，沒有詳盡的搜尋字眼便不可能成功。現在的搜尋器，卻像你肚裡的蛔蟲，你隨便輸入一兩個搜尋字眼，可能也找到你想要的東

西。因此，起底的第一步，就是在搜尋器輸入目標人物的資料。資料不一定是全名，可能是網名、暱稱……只需輸入一些關鍵字眼，搜尋器便會找到一些相關的網頁。

值得一提的是，搜尋是否成功，視乎當事人有否好好保障自己的個人資料。如果你的 Facebook 私隱設定不夠嚴密，把個人資料全部公開，網誌又披露每天生活細節，那麼起底者也省下大量工夫，「Google 一下」、按幾下搜尋器便能找到你的所有資料了。

社交網絡（例如 Facebook）、個人網頁、網誌本來是好東西，這些方便的工具可以讓你認識新朋友；另外，在網絡世紀來臨前，我們會把日記藏在抽屜，相簿則放在家中某處封塵，但現在日記和照片都放上網，人人都可以看，這樣有其好處，但亦潛藏危機。我們上載個人資料前，應先了解風險，考慮一下：是否必須上載詳細資料？不放全名，只放暱稱可以嗎？公布自己在哪家公司工作、工作性質如何，對認識新朋友真的有幫助嗎？

上載到社交網絡、網誌的資料，用搜尋器便能輕易找到，所以我們有必要思考以上問題。各位在家可以嘗試在搜尋器輸入自己的姓名、暱稱、英文名、公司名稱、學校名稱等等，可能也會找到自己的資料！如果我們不保護個人資料，起底者可能不消五秒便大功告成了。

也有人在不同網站會有不同態度。舉例說，他們上高登討論區時，較擔心自己成為起底目標，所以較少披露個人資料，避免他人猜到自己是誰。然而，到了 Facebook，他們則持較開放態度，以為 Facebook 沒有起底者，便可以公開較多資料。到了其他討論區，態度又更開放，例如那是分享讀書往事的討論區，就公開了自己以往就讀的學校。如是者，他們把不同資料放在不同網站。但網民素來擅長資料搜集，就像警察偵查案件一樣，利用搜尋器等工具，可以在不同網站找出蛛絲馬跡，然後像砌圖一般，砌出完整的個人資料。有人認為只要不把個人資料集中於同一網站，便足以保障資料安全，但有心者就是懂得在不同網站找出所有資料。我們必須記住這一點。

第二個起底方法，就是利用手機應用程式的**臉孔識別軟件**。現在流行的智能手機備有攝影功能，又有程式可連上 Facebook 等社交網絡，而臉孔識別軟件，可以根據手機裡儲存的照片，找出相中人的社交網絡帳戶。於是，你在街上被拍下照片後，Facebook、Twitter 的帳戶也可能被人發現。如果你在這些網站公開了個人資料，資料便公諸於世。

臉孔識別軟件面世時，也有專家指出這軟件功能太強——拍照者可能不認識被拍

照者，卻可以找到對方的 Facebook、Twitter 等——擔心軟件被不法之徒利用，侵犯陌生人的私隱。不過，話又說回頭，如果我們好好保障自己的資料，好好利用社交網絡的私隱設定，把個人資料封鎖起來，便不用太擔心臉孔識別軟件。

第三種起底手法，則是**社交工程**。首兩種起底方法都利用了工具，但在社交工程中，起底者直接誘騙受害人透露密碼或個人資料。舉例說，討論區一定會有 PM（Private Message，私人訊息）功能，而起底者可能會 PM 受害人，訛稱自己對受害人提及的話題感到興趣，例如希望購買受害人出售的貨品。然而，PM 寄出者真正感興趣的，只是對方的個人資料，所以可能會不斷誘騙對方說出個人資料，例如堅持以電話聯絡，或要求受害人說出密碼。更有甚者，起底者可能會聯群結隊，每人詢問不同的問題，索取不同的資料，然後集腋成裘，拼砌成完整的檔案。

不過，誘騙他人說出個人資料，有機會觸犯法例，所以也不是所有網民都敢於冒險。因此，又有第四種方法，即「**人肉搜尋**」。這方法不涉及誘騙，只是採用「人多好辦事」的原理。一人之力畢竟有限，於是有心者便在討論區召集大量人馬（這在討論區是不難辦到的），大家一起行動。起底人數由一人暴增至成千上萬人，即使大家也只是用搜尋器，起底的成功機會也會倍增。

「人肉搜尋」厲害之處，就是在聚集了一定數量的人馬後，就不一定只能用搜尋器了。香港只是彈丸之地，如果大量網民都希望追查一個人的底細，其中一個網民可能正正認識目標人物！目標人物可能是網民的朋友、鄰居、同事、同學……只要有足夠多的人參與「人肉搜尋」，總會有人認識目標人物。

「人肉搜尋」如此厲害，實在很難躲避。不過，起底者需要發動「人肉搜尋」，代表你已經做了不少保密個人資料的工夫，他以一人之力無法起底，才要依靠他人。而且大家也無須過分擔憂，因為要發動大量網民免費為你追查一個人的底細，其實相當困難。即使有很多人找來不同的資料，發起人仍要花費時間、精神以整合資料，殊不輕鬆。

第五種起底方法，是靠網民在討論區「**出賣朋友**」。對於這做法，各討論區態度迥異。高登討論區並不贊同此做法，所以不會出現這情況。贊同此做法的討論區，可能有「出賣朋友專區」，鼓勵網民張貼朋友或同學的照片，而且相中人的樣貌必須清晰可見。

雖然這些討論區只是主動呼籲網民公開他人照片，並不鼓勵公開其他個人資料，但網民往往不會如此乖巧，經常同時公開照片及資料。有了這些「出賣朋友專區」，起底者就可以在這些專區表示希望知道某人的資料，呼籲認識該人的網民

「出賣朋友」。

第六種起底手法，是使用**駭客軟件**。使用這方法的人較少，因為這是犯法的，而大部分網民都了解法律，不會以身試法。不過，如果起底者電腦知識較高或擁有特殊目的，便會使用各種各樣的駭客軟件：以截聽軟件為例，可以在目標人物於網上向朋友傳送資料時，讓駭客截取並閱讀該些資料。

這種手法的電腦知識要求較高，又違反法律，因此在香港並不普遍；但仍然值得一談，因為部分駭客軟件必須先安裝在受害人的電腦，才能生效。這提醒我們：千萬不要胡亂安裝程式。比較可能帶有駭客程式的，通常是非法軟件，而且會給你一些甜頭，例如讓你免費看電影或聽音樂。雖然不是所有這類軟件都帶有駭客程式，但大家務必小心。較穩妥的做法是只安裝正版軟件。

另一種可以用以起底的，是**檔案分享軟件**。與駭客軟件不同，檔案分享軟件的設計原意是便利網民，提供合法點對點傳送檔案的途徑。不過，Foxy 等檔案分享軟件不時洩漏用戶個人資料，相信大家從報章亦略有所聞。因此，使用這些軟件時，我們必須了解小心操作其私隱設定，不然軟件可能會把整部電腦的檔案都分享出去，連你不想與人分享的資料都公開，讓人予取予攜。

值得一提的是，萬一你不小心分享了某些不想公開的資料夾，有心者可能會利用 Foxy 等軟件，搜尋你電腦中的檔案。有些人記不住自己所有帳號的密碼，便把密碼儲存在某檔案，檔案名稱可能還叫「password」、「pwp」。這些檔案正是有心者第一個搜尋目標，一被找到，你的密碼便被人知道了。

不是要迴避安裝檔案分享軟件，但大家必須謹慎一些，不要把不想公開的檔案都分享出去。

最後，起底還可以透過**不誠實的電腦維修員**進行。大家把電腦拿去修理，自然希望把壞掉的部分修理好。但有些維修員不但修理壞掉的部分，還會偷取完好的檔案。偷取電腦檔案與偷取其他東西不同。如果有人偷走了我手上的咪高峯，我可以看見咪高峯消失了；但電腦檔案很容易就可以複製，即使被偷取了，你也未必知道。

因此，大家把電腦拿去修理的時候，一定要小心。平日我會把所有資料儲存於外置硬碟，因此電腦並無任何資料，拿去修理也不怕洩密。儲存資料的硬碟也設置了密碼，所以即使硬碟被偷，資料也不會外洩。把資料分散儲存比較穩妥，而如果某些資料特別重要的話，便要再用另一硬碟備份了。

網絡密碼安全小提示

說了那麼多起底個案，大家應該明白現實世界與網上世界之間的連繫有多緊密。為防止自己成為起底的受害者，我們也要做足預防工作。

首先，就是**設定一個好密碼，避免使用常見而容易猜中的密碼模式**，例如：

- ✧ 順序數字（如 123）
- ✧ 順序的全小寫字母字母（如 abc）
- ✧ 生日。有人計算過，以自己或親友的生日日期作密碼的話，可能出現的六位密碼只有 446,400 個，速度較快的計算機用十秒就可以破解了。
- ✧ 姓名。即使你使用中文名拼音作密碼，破解者也備有字典，記錄著姓氏的各種拼法，逐一嘗試。因此，不要以為拼音不是英文字，就沒那麼容易被猜中。
- ✧ 電話號碼
- ✧ 電腦常用字（如 password、window）
- ✧
- ✧ 「有意思」的密碼，例如 520（我愛你）、1314（一生一世）。香港人似乎特別愛用這種密碼，以為只有聰明的自己才會想到，但其實人人也想得到的
- ✧ 與帳號一模一樣的密碼。別以為這很荒謬，真的有人為方便記憶而如此設定的。
- ✧ 名字加數字

有一些破解密碼的程式，會針對以上常見的密碼模式，逐一試探。如果可以避免使用以上模式，密碼被破解的可能性便會降低，最少也要耗時較久。有些網站只容許你輸入十次密碼，十次都不對就不可再試，但如果你的密碼簡單得十次之內就可猜中，這也是沒用的。如果沒有限制輸入次數，簡單的密碼就更容易被破解了。

現時的破解密碼程式非常強大。以英文單字為密碼，計算機用 111 秒就可破解；以八位數字為密碼，破解時間也是不到三小時；五位以下的字母數字混合密碼，約用 25 分鐘就可破解。

約是 2009 至 10 年的時候，駭客攻擊某大型網站，盜取 3,200 萬用戶的密碼並加以分析，發現最常用的密碼就是 12345、123456、password、123456789、iloveyou、網站名稱等等。香港也進行過類似統計，得出香港「最爛密碼」：123456、password、000000、網站名稱、46709394（諧音「死佬出來攪三攪四」）、123321、5201314、abc123、iloveyou、30624700（林子祥《數字人生》歌詞）、qwerty（鍵盤左上角的英文字母）……如果在座有人使用這些密碼，便要小心了，不要以為

只有自己想到這些密碼呢。

另外，建議各位**在不同網站使用不同密碼，各個密碼亦應有信任等級之別**。如果是銀行密碼，就要用最難被猜破的，討論區密碼反而可以比較簡單。討論區密碼失竊事小，如果駭客取得討論區密碼後，連你的銀行帳戶也可以登入，那就大事不妙了。

設定了這麼多密碼，也要記著剛才討論 Foxy 時提及的：**不要把密碼儲存在同一檔案，即使儲存了，也要多重加密、備份**，那才比較穩妥。

如何保障個人資料避免被網上被底

保護個人資料方面，最好的做法還是**避免在網上公開自己的資料**。資料一旦公開，就很難收回了。我們應了解公開資料的危機，先確定有公開的必要，才透露自己的資料。

另外，被起底者多是做了一些在多數網民眼中很過分的事情，才會成為網上短片的主角，激起公憤而被起底。不少人都在網上說自己被欺負，希望網民幫忙找出對方的底細，卻不受理會。「人肉搜尋」雖然厲害，卻不是可以輕易發動的。因此，**注意自己在現實世界的行為，也可以減少被起底的機會**。我們應**避免惡搞、騷擾別人**。

最後，大家參與起底之前，最好思考一下自己是否被利用。起底目的有很多，你認同這次起底的目的嗎？記著**三思而後行，不要太容易被煽動**。

資料來源：

- 香港網絡大典
- 《釐清「網絡欺凌」的真正涵義》，香港樹仁大學新聞傳播學系副教授宋昭勛