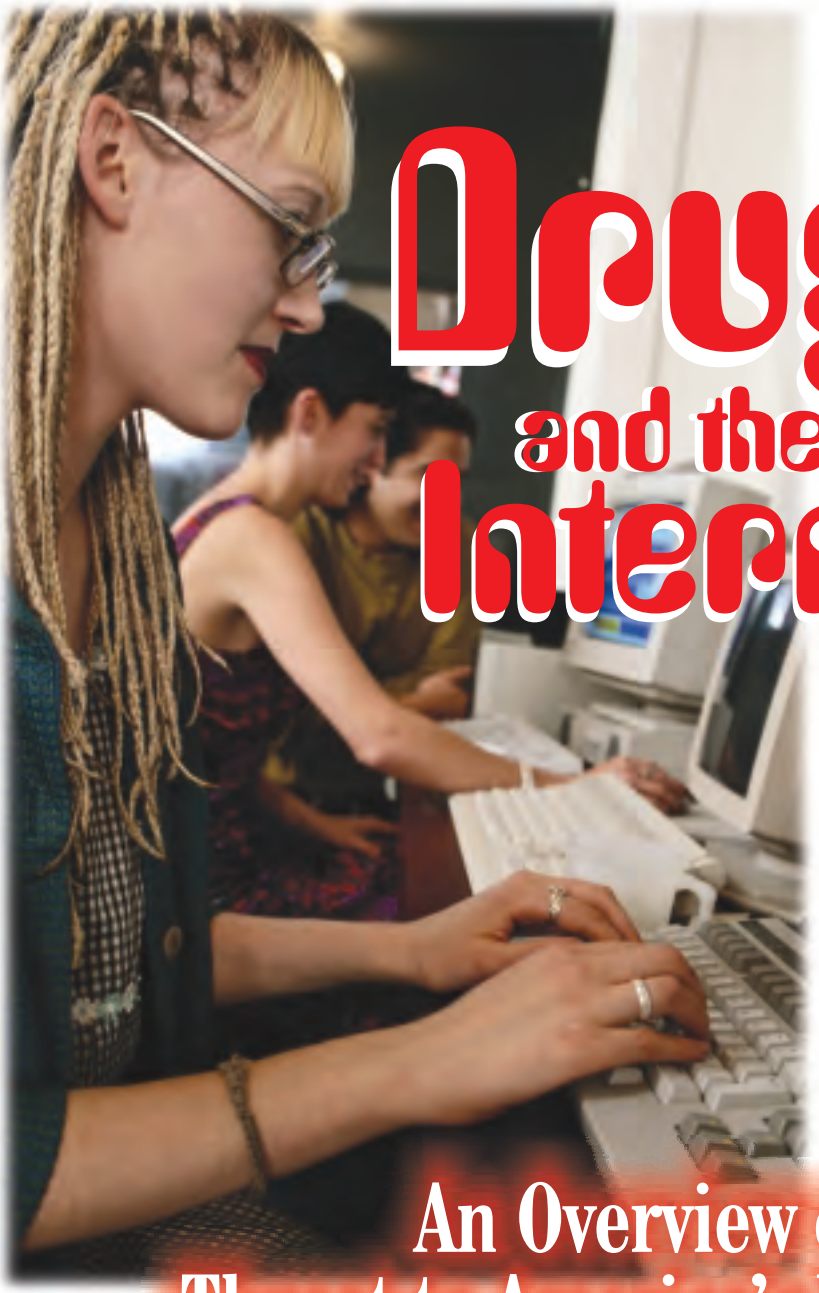
December 2001



© Photodisc

Drugs and the Internet

An Overview of the Threat to America's Youth

U.S. Department of Justice
National Drug Intelligence Center

Product No. 2002-R0430-001
December 2001

Drugs and the Internet:
An Overview of the Threat to America's Youth

National Drug Intelligence Center
319 Washington Street, 5th Floor
Johnstown, PA 15901-1622
(814) 532-4601

Executive Summary

This report is an overview of the threat that certain Internet websites pose to adolescents and young adults in the United States. This preliminary baseline is intended to assist policymakers in countering this threat to America's youth. This report focuses on websites that promote or facilitate the production, use, and sale of *MDMA, GHB, and LSD*, three significant "club drugs." A full strategic assessment addressing the Internet drug threat in greater depth will follow this overview report. In producing the strategic assessment, NDIC will coordinate with the Drug Enforcement Administration and other federal law enforcement agencies as appropriate. The assessment's descriptions and analysis will provide a more comprehensive view of the status and magnitude of Internet activity and will be provided to national-level policymakers and law enforcement personnel to further their understanding of this threat.

An increasing number of adolescents and young adults in the United States, with ready access to information, services, and contacts through the Internet, are contributing to the U.S. drug problem by engaging in various types of illegal and harmful behavior. Internet use has grown rapidly in this country, and an estimated 85 percent of Americans aged 12–24 now use the Internet regularly. The large number of younger Americans accessing the Internet has encouraged legitimate and illegitimate entrepreneurs—including drug offenders—to market and sell their products to young people through this powerful medium. Many websites, newsgroups, bulletin boards, and chat rooms promote the drug culture by providing a wide variety of information on drugs and drug paraphernalia. Law enforcement efforts in identifying illegal Internet activities are a challenge because information can be exchanged and sales consummated quickly and with relative anonymity. Drug offenders are increasingly taking advantage of sophisticated encryption and security technologies to hide their actions and identities, and much of the activity that can be discovered appears to be constitutionally protected as free speech.

Information about the production, use, and sale of MDMA, GHB, and LSD is widely available on the Internet. Although most MDMA production now occurs outside the United States, the potential exists for expanded production in the country, including by American youth. GHB is increasingly being produced in the United States, and many young producers use recipes they find on the Internet. Young persons who use "club drugs" or are contemplating their use can readily access information about them on Internet websites, including explanations of drug terminology, methods of use, and dangers associated with use. Many of these websites popularize and glamorize drug use, and others implicitly promote use and experimentation. Because MDMA, GHB, and LSD are Schedule I controlled substances, their sale is not often advertised on the Internet. However, suppliers and customers often meet through Internet bulletin boards and chat rooms and arrange the sale of drugs or chemicals, which are then shipped to the customer for an agreed price.

Project Background

Focus

The National Drug Intelligence Center (NDIC) will assess the use of the Internet to facilitate the production, sale, and use of drugs and drug paraphernalia. NDIC has drafted a set of specific and focused intelligence requirements, which define the project scope. The assessment will concentrate on Internet websites that do the following:

- Display information intended to facilitate the production or cultivation of federally scheduled, nonprescription drugs
- Display information intended to facilitate the use of federally scheduled, nonprescription drugs
- Facilitate the sale of federally scheduled, nonprescription drugs and drug paraphernalia

To focus on the issue of drug activity among adolescents and young adults in the United States, this initial report addresses the requirements as they pertain to three significant "club drugs": *MDMA, GHB, and LSD*. NDIC's follow-on strategic assessment will address the requirements as they pertain to these and other drugs in greater detail.

Internet Parameters

This project examines *registered domains* (web addresses controlled by laws of the registering country and sold to webmasters for a fee, usually annual) and *subdomains* (subsections of the registered domain that a webmaster, in turn, allows other webmasters to use for a fee or for free). *Newsgroups* and *open bulletin boards* are included in the scope.

To provide context, this report discusses, when relevant, the threat posed by use of email, chat rooms, list servers, and non-website communications such as File Transfer Protocol (FTP) and Telnet. However, these media are not included in the project scope because they are difficult to monitor and virtually impossible to quantify given their vast use and the fact that tracking is negligible and can be done only at the individual server or Internet Service Provider (ISP) level.

The project scope includes both domestic- and foreign-based websites, because the Internet is a global platform virtually unconstrained by boundaries and jurisdictions. However, the scope is limited to websites in English, because expanding the scope to websites in other languages would have necessitated the use of translators, both to develop Internet search strings with foreign words and phrases and to collect pertinent information from the Internet and other sources. Limiting the scope to English websites is not expected to significantly affect the project's findings.

Research Methodology

When conducting research in support of this project, NDIC has used a "non-investigative" and "non-intrusive" approach. To ensure compliance with the Privacy Act, NDIC did not collect information on specific individuals. In addition, NDIC has collected only publicly available information and has not engaged in communication with persons or websites. This conservative research approach will continue as the project progresses.

The Internet: The Emergence of an Information Superhighway

The Internet[1] has revolutionized communications worldwide. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard to geographic location.[2] Variously referred to as the National Information Infrastructure or the information superhighway, the Internet serves today as the nation's primary medium for the exchange of news, mail, and general information, and is rapidly becoming a principal hub of commercial and banking activity as well.

In 1962, the genesis of what later became the Internet was conceived as a decentralized computer network, able to withstand a nuclear attack and ensure the survival of military command and control systems. The prototype network took 7 years to develop. In 1969, the Internet was born as an aggregate of four computer networks located at three universities and one research facility. Over the next 30 years, the Internet grew exponentially. There were over 100 million Internet users in the United States in 2000, and that number is expected to reach 177 million in the United States and 500 million worldwide by 2003. Electronic commerce has emerged as a new sector of the global economy, accounting for greater than $100 billion in sales during 2000, which is more than double the amount in 1999. By 2003, electronic commerce is anticipated to exceed $1 trillion.[3]

Minors and young adults have become the largest segment of the U.S. population with Internet access. A 2000 study released by the Ipsos Reid Group showed that 85 percent of Americans aged 12–24 used the Internet regularly, compared to 59 percent of the rest of the adult population. The 85 percent participation rate among U.S. youth was higher than the rate in nine other industrialized countries.[4] About 30 million American children under 18 currently use the Internet, and more than 40 million are expected to be online by 2005.[5]

---

[1] The *Internet* refers to the global information system that (1) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (2) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (3) provides, uses, or makes accessible, either publicly or privately, high-level services layered on the communications and related infrastructure described herein. Source: Barry M. Leiner et al., *A Brief History of the Internet*, URL: <http://www.isco.org/Internet/history/brief.html> accessed 3 April 2001. The World Wide Web, the set of all websites in the world, rides on the Internet.

[2] Barry M. Leiner et al., *A Brief History of the Internet*, URL: <http://www.isco.org/Internet/history/brief.html>, accessed 3 April 2001. Verbatim.

[3] National Institute for Government Innovation, International Summit on Cyber Crime, promotional material, received by NDIC in February 2001.

[4] Ipsos Reid Group, *American youth global Internet pacesetters*, URL: http://www.canalipsos.com/english/articles_gb/0005/y_Internet.htm, accessed 3 April 2001. American youth surpassed those in Australia, South Korea, the United Kingdom, Italy, Germany, Spain, France, Japan, and Argentina in Internet use.

[5] Grunwald Associates, *News Release – Children, Families, and the Internet*, URL: http://www.grunwald.com/survey/newsrelease.html, accessed 10 April 2001.

The Nature of the Threat

The Internet differs from other information media in part because information can be disseminated at will to a specific or wide audience; because information exchange occurs very quickly, easily, and inexpensively; and because information providers and users can often protect their privacy. The openness of the Internet, its global reach, and its ease of access have encouraged many individuals and groups to use the medium to promote or facilitate illicit drug activities. The threat perpetuated by these individuals and groups as it relates to adolescents and young adults in the United States can be defined and circumscribed by the following:

> **The threat to adolescents and young adults in the United States accessing the Internet consists of information, disseminated by drug offenders or others, that is intended to facilitate the production, use, or sale of federally scheduled, nonprescription drugs. Information facilitating production includes explanations of equipment or other resources needed or processes used. Information facilitating use includes explanations of the nature, effects, or administration methods of drugs. Information facilitating sales includes explanations of how or where drugs may be obtained or mechanisms allowing for online purchase of drugs.**

The Information Purveyors

Information available on the Internet is generated by individuals and groups with varied agendas and motivations. Sources of information include the following:

- *Drug offenders* use the Internet to expand their customer base by inducing a young audience to engage in illegal or harmful behavior. These drug offenders may act either singly or as part of a conspiracy. They also may use the Internet to induce a young audience to engage in criminal activities related to drug trafficking, as well as other offenses such as credit card fraud and other financial crimes.
- *Drug-culture advocates* are chiefly interested in expanding the size of the community to both legitimize their activity and increase pressure on lawmakers to change or abolish drug control laws. These individuals and groups share information via the Internet to demonstrate the ease with which drugs can be produced, trafficked, and obtained. They may or may not be drug offenders themselves and may or may not induce others to engage in harmful or illegal behavior, but they often glamorize drug use and extol the virtues of illegal substance abuse.
- *Advocates of an expanded freedom of expression* are purveyors of information with yet another agenda. These individuals and groups publish information on the Internet to push the boundaries of self-expression and the First Amendment. The information they provide may induce minors and young adults to break drug laws or to become a danger to themselves or to others by abusing illegal drugs.
- *Anarchist individuals and groups*, who protest against or seek to abolish current legal, social, or economic structures, disseminate drug information on the Internet to advance their cause by promoting countercultural behavior. They may induce others to disobey drug laws as a part of their worldview, or drug abuse may be an implied undercurrent of their lifestyle. The presence of these individuals and groups on the Internet is a known fact.

- *Other lawbreakers* use drug websites to encourage minors to perpetrate crimes unrelated to drugs or to lure them into being victims of crime. *Pornographers* and *pedophiles* would fit this threat group.

The Location of the Threat

The unrestrained nature of the Internet makes the threat's location a very complex matter. Potentially harmful information contained on websites may be static one moment and moving across the network the next. Information transmitted over the Internet can move in whole or in part through a series of interim points in very rapid succession. This state of flux is a function of the architecture of the Internet and of the manner in which the information itself is physically subdivided for transmission.

Large web-based documents are not transmitted as single units through the Internet. Instead, internetted computers break down information into smaller units called *packets*, to speed their handling and delivery. Generally, control devices called *routers* direct these packets by identifying the shortest or least congested pathways between the origin and destination. Once packets leave a router, they travel through multiple paths on the Internet *backbone* before being reassembled at the *ISP's server* for ultimate delivery to the *end user*. A personal computer (PC) or other Internet-ready device, equipped with the appropriate communication software and hardware, downloads the information and then interprets and displays it through a *browser* (e.g., Internet Explorer or Netscape Navigator) or stores it for later access by other software applications. All these processes, occurring "behind the computer screen" as it were, are transparent to the end user.

There are at least three physical points on the Internet where the location of potentially harmful information can be pinpointed:[6]

- At the *insertion* point, where the website's creator originates the information and uploads it to the World-Wide Web. This insertion point usually corresponds to the personal computer system where the author designed the website.[7]
- At the point where the website is stored, or *hosted*—typically, at the web server of the user's ISP, or at a third-party web hosting company.
- At the point where the *end user receives the information*—typically, at the end user's personal computer, Internet appliance, or other Internet-ready device.

Identifying the *insertion point* and the *hosting point* can be difficult, because geographical addresses and Internet addresses of websites can be obscured through a variety of software or hardware techniques. However, if a website containing potentially harmful information is open and accessible to all Internet users, then the geographical location of the router supporting the website can be pinpointed by tracing the path the information stream follows between its origin

[6] Only for information that is meant for general, unsecured, and unobstructed dissemination.
[7] If the user is using an "Internet appliance" instead of a PC to access the Internet, there will be no legacy data (files or fragments of files created by the computer while processing any kind of information) at the insertion point because an "Internet appliance" lacks a hard drive.

and destination points. This trace will yield the specific location of the router nearest to the web server hosting the website that contains the potentially harmful information. The router's location therefore will indicate the general geographical vicinity of the web server, since routers support servers in designated geographical regions.

Identifying the point where the *end user receives the information* would involve more intrusive means of information collection, and even then results may vary according to how the user accesses the Internet. If a PC were used, its location could be ascertained by examining the ISP's customer records (which would require a subpoena) or by using a Title III wiretap (which would require a court order). Establishing that the end user's system had been the recipient of such information could be done using computer forensic searches (which would require a search warrant). However, identifying the right system, at the right place, and at the right time using any of these methods would in most cases require a human intelligence tip or a security lapse on the part of the end user.[8]

Identifying Individuals/Groups

The ability of drug offenders to successfully evade law enforcement is determined partly by their level of technical sophistication, which includes their ability to hide, mask, and move sites. It is very possible that the individuals/groups most easily identified and caught by law enforcement are also the least technically savvy or "Internet smart." They also may be the ones involved in less significant drug activities; offenders with more to lose are likely to use more advanced methods to "cover their tracks."

Drug offenders are now using the same encryption and security technology that protects Internet commerce to keep drug activities hidden from investigators' eyes.[9] New software and hardware tools recently developed by the computer industry allow individuals and groups to impede law enforcement attempts to penetrate their communications. These developments include anonymous email remailing, encryption software, and Internet telephony.[10]
Most individuals maintaining pro-drug websites provide a disclaimer, which they believe shields them from law enforcement scrutiny. When these disclaimers appear on websites that contain a great amount of information promoting the drug culture and the use of illegal substances, it can be inferred that the disclaimers lack sincerity.

In many cases, drug offenders operate websites on subdomains, space which registered domain owners give or lease to others for personal use. Drug offenders also operate on domains that are registered in another country, which means their websites are not subject to U.S. law. However, individuals and groups that operate websites on their own *registered domains* often can be identified. To acquire a registered domain, a person must provide some personal information that

[8] If the end user were using a stationary Internet appliance, there would be no legacy data in the user's equipment to search forensically. Also, if the user were accessing the Internet though a mobile device, especially one attached to a cellular modem, locating the end user would be extremely difficult, requiring very specific information developed through case work and the use of advanced technology.
[9] Jim Krane, "Narcs Online: Cops Chase Drugs Onto the Net," URL: <APBNews.com>, accessed on 22 September 1999.
[10] *National Gang Threat Assessment*, National Alliance of Gang Investigators Associations, February 2000, p. 16.

may include name, business, address, phone number, and credit card number. This information, which is posted publicly on the Internet, can help law enforcement identify or physically locate a person, assuming the information is not fictitious. Registered domains have to be paid for, usually on an annual basis, and payments usually provide a direct link to a person.

Drug Production and the Internet

The Internet provides access to a vast amount of information on drug production, including processes, recipes, ingredients, and substitutes, and this information is readily available to minors and young adults in the United States with Internet access. Misinformation is fairly common and can lead to serious injury, illness, or death.[11] Production equipment also is advertised widely, and chemicals needed in the production process are available as well.[12] Even the most inexperienced drug producer can easily obtain the instructions, ingredients, and equipment needed to synthesize many illegal drugs in a kitchen, bathroom, or basement laboratory.[13]

MDMA

Although most MDMA (3,4-methylenedioxymethamphetamine) is produced outside the United States,[14] the potential exists for expanded production in the country, including by American youth. MDMA production is somewhat difficult but still within the capabilities of many young people, assuming they can obtain the necessary precursor chemicals.[15] MDMA is synthesized from several precursor chemicals, most of which are federally controlled. Producers can use the Internet to identify suppliers of these chemicals and to obtain recipes and instructions on MDMA production. Many websites simply post a description of the MDMA production process published by Alexander and Ann Shulgin in their book *Phenethylamines I Have Known And Loved: A Chemical Love Story* (a.k.a. "PIHKAL"), or else provide a hyperlink to a website that posts the description. Alternate methods for synthesizing MDMA and its analogs, such as MDA, are easily found on the Internet.

The Drug Enforcement Administration (DEA) reports the arrest of two chemistry doctoral students, one in Georgia and one in Arizona, who used instructions from the Internet to produce MDMA, methamphetamine, and precursor chemicals. The students communicated with each other about their progress via email.[16]

[11] "Internet Highway: Road to Enlightenment or Danger?" NDIC, 23 August 2000.
[12] The chemical industry, which incurs an enormous cost savings in processing orders online, expects 80% of its business will be on the Internet by 2005 ("Internet Resources for Clandestine Drug Manufacture," presentation at National Chemical Initiative Training, Drug Enforcement Administration (DEA) Western Lab senior chemist, September 11-12, 2000).
[13] "Internet's easy access feeds drugs to 'pill-popping culture'," *Washington Times*, 21 February 2001, p. A11.
[14] *Joint Assessment of MDMA Trafficking Trends*, 2000-L0352-001, NDIC, July 2000.
[15] DEA chemist interview, conducted by NDIC, 10 May 2001. MDMA production is generally considered to be more difficult than methamphetamine production.
[16] *Drug Intelligence Brief: Drug Traffickers in Cyberspace*, DEA Headquarters Intelligence Division, December 1999.

GHB

GHB (gamma-hydroxybutyrate) is increasingly being produced in the United States,[17] and the production process is considered to be very easy.[18] The precursor GBL (gamma-butyrolactone), although a controlled chemical,[19] can be purchased over the Internet. The recipes available on the Internet for GHB production are not nearly as standardized as those for MDMA. Incorrect information is relatively common, and as a result, some sites explain how to tell the difference between "fake" and "real" GHB recipes. Some GHB information is exchanged on pro-drug and fitness websites, including information on production processes and ways to obtain GHB production kits and chemicals.

Newsgroup posting: "I need some answers in a hurry. 3 DEA agents showed up at my door today with a box which they say contained GBL addressed to me….First, is GBL illegal to receive in the mail, Second, Can they trace it to me, and finally if they can what should I say."

Newsgroup responses: "If you bought it as a cleaner, nail polish remover or wood stripper you can claim ignorance to it being a controlled substance." "…try to play ignorant and say that you have a lot of furniture you're trying to refinish and needed some stripper that wasn't toxic….get rid of any bottles of NaOH[20]….that way, they wouldn't have hard evidence in case of a search that you were trying to synthesize GHB."[21]

LSD

LSD (lysergic acid diethylamide) synthesis is a complex chemical procedure that requires the knowledge and skills of a trained chemist.[22] However, recipes for making LSD still are readily available on the Internet, often via hyperlinks to instructions from another Shulgin book, *Tryptamines I Have Known And Loved: The Continuation* (a.k.a. "TIHKAL"). LSD production instructions often warn that production should be undertaken by experienced chemists only and that the precursor and essential chemicals are difficult to obtain. Other sites, however, provide instructions for making LSD using substances that contain the LSD precursor ergine (lysergic acid amide).[23]

---

[17] *National Drug Threat Assessment 2001 – The Domestic Perspective*, NDIC, October 2000; Terrance Woodworth, former Deputy Director, Office of Diversion Control, DEA, Testimony before the House Commerce Committee, Subcommittee on Oversight and Investigations, 11 March 1999.

[18] DEA chemist interview, conducted by NDIC, 10 May 2001.

[19] Controlled as a List I chemical in legislation signed by the U.S. President on February 18, 2000 ("GHB: The Stone Cold Truth – Laws, Legislation, Legalities", www.ashesonthesea.com/ghb/laws.htm, 21 December, 2000).

[20] The chemical abbreviation for sodium hydroxide.

[21] URL: <alt.drugs.ghb> newsgroup, actual message posted at URL: <http://groups.google.com/groups?hl=en&lr…ic=1&th=e82ade7b44f43ead&seekd=902943420>, accessed on 12 April 2001.

[22] DEA chemist interview, conducted by NDIC, 10 May 2001.

[23] *Drug Identification Bible*. 4th ed. Edited by Tim Marnell. Grand Junction, CO: Amera-Chem, Inc., 1999.

Drug Use and the Internet

The Internet has a vast repository of information on the effects of drug use and co-use, as well as explanations of drug terminology, methods of administration, and warnings.[24] Minors and young adults in the United States can find information about any drug that they are using or thinking of using on Internet websites. Many of these websites openly promote drug use, others glamorize the drug culture and thereby implicitly promote use and experimentation. More and more websites are being established to cater to the youth party scene, serving as pointers to the next rave or nightclub gathering where illegal drugs are often sold and used.[25]

MDMA

MDMA use is promoted and glamorized on many pro-drug websites and bulletin boards, and discussions of the administration of MDMA by itself or in combination with other drugs are readily available. Drug legalization and club/party websites often describe MDMA as a relatively benign drug with few negative side effects, while at the same time providing warnings to potential users. These warnings include the fact that harmful substitutes are often marketed as MDMA, and that MDMA use can result in dehydration. Users are encouraged to test pills before ingesting them and to properly rehydrate themselves afterwards. Websites occasionally give information on vitamins and food supplements that some MDMA users believe are helpful in preventing negative side effects. Most websites promoting MDMA use also provide hyperlinks to other sources of information on the Internet.[26]

> Newsgroup posting: "It's like warm electricity flowing through your whole body. You feel relaxed, connected to everyone around you, empathetic, and usually like dancing. :) Every touch is an experience….Your first time, it could last anywhere from 6-8 hours, or hell, even more, if you use 5-HTP and the like (myself or someone else could post instructions on that if you are interested). In most places, the average cost is $20 per pill, but as you do it more, you will probably get more 'connected' and be able to get it for less (I've gotten it as low as $3 before… well worth the drive!!). When you do it, be SURE you stay hydrated, and take time to cool off if you start feeling way too hot. Dehydration and overheating are the main dangers associated with E."[27]

GHB

GHB likewise is portrayed as a relatively benign drug on many Internet websites, usually with the caveat that correct dosing is extremely important. Addiction and the possibility of overdoses and death are generally downplayed, and the use of GHB in drug-facilitated rape is often dismissed as media hype. On some pro-drug and fitness websites, GHB is promoted as an athletic performance enhancer, an antidepressant, and a sleep aid. These websites also discuss using GHB substitutes, such as "Renewtrient" and "Verve," that are said to mimic the effects of

[24] "Internet Highway: Road to Enlightenment or Danger?" NDIC, 23 August 2000.
[25] *Quarterly Trends In The Traffic Report, First Quarter FY 2001*, DEA Houston Field Division.
[26] "Users Report the Agony of Ecstasy," NDIC, 16 November 2000.
[27] URL: <alt.drugs.ecstasy> newsgroup, actual message posted at URL: <http://groups.google.com/groups?hl=en&lr…ic=1&th=a64dcafe6526c7b2&seekd=902932379>, accessed on 12 April 2001.

GHB. However, there are some popular pro-drug websites that more accurately describe the dangers of GHB use and do not openly promote its use.

> Newsgroup posting: "I take two teaspoons and feel very calm and a little euphoria…three teaspoons makes the feeling go up a pretty good notch to slightly drunk and causes me to get very communicative…I like to get sincere and deep with those around me…One thing I have noticed is how vivid my dreams get while or after taking G…No kidding…I almost feel as though the dreams are actually happening."[28]

LSD

Extensive information on the use of LSD is available on the Internet. Historical information on LSD use in the 1950s and 1960s is found on many sites, including information on the experimental use of the drug on patients treated by psychiatrists and mental health professionals during those years. Although information available on LSD websites often indicates the drug has no potential for physical or psychological addiction, most sites warn that users may experience "bad trips" and recommend using LSD in familiar settings in the company of trusted friends. Information about how much LSD to take is frequently presented, including the differences between psycholitic dosing (taking 75–200 micrograms) and psychedelic dosing (taking 500 micrograms or more). Discussions about the psychological dangers, flashbacks, and insomnia often associated with LSD use are common as well. Some websites list other hallucinogens that produce effects similar to LSD without the risk of flashbacks. Internet bulletin boards provide an interactive, conversational setting for individuals to share LSD "tripping" experiences.

> Newsgroup posting: "i was 15 when i tripped my first time. i got a red gel tab off some kid it school….anyway, I took it in school, 8th period, and it really had kicked in when i got home….i was standing atop a desert plateau, singing to thousands of pissed off monsters….i sat watching the beautiful hologram-ish images appear before me. i saw Grim Reaper-like images, and lots of screaming mouths that appeared to be projecting at me. then i went to dinner with my parents."[29]

Drug Sales and the Internet

Legal drugs are widely advertised on the Internet and can be ordered through websites. Controlled substances are openly advertised less often, but suppliers often arrange sales with customers via bulletin board discussions carried on in coded language, and then ship drugs to the customer by mail for an agreed price. Law enforcement reports indicate that the source of much of these illegal drugs is foreign.[30] Wholesalers sometimes, and perhaps often, act as middlemen between customers and suppliers in these transactions, and because the customer, supplier, and

[28] URL: <alt.drugs.ghb> newsgroup, actual message posted at URL: <http://groups.google.com/groups?hl=en&lr…ic=1&th=da7e85012da5076&seekd=903352332>, accessed on 12 April 2001.

[29] URL: <alt.drugs.lsd> newsgroup, actual message posted at URL: <http://groups.google.com/groups?hl=en&lr…ic=1&th=bfc5173b54910c57&seekd=939409907>, accessed on 12 April 2001.

[30] *Trends In The Traffic, 1st Quarter 2001*, DEA Phoenix Field Division; *Trends In The Traffic, 1st Quarter 2001*, DEA St. Louis Field Division.

wholesaler usually never meet, the threat of exposure and risk is reduced.[31] Minors and young adults searching for user or wholesale quantities of drugs can easily find suppliers on the Internet. Drug production equipment, chemicals, and other paraphernalia are readily obtained through online stores.[32]

MDMA

MDMA is a Schedule I drug under the Controlled Substances Act (21 U.S.C. **§** 812), and selling the drug over the Internet is prohibited. MDMA sales, therefore, do not commonly occur via the Internet, but transactions often are arranged through Internet communications. Negotiations most often are held on bulletin boards where individuals post messages and wait for replies. MDMA producers also use these bulletin boards to locate suppliers of illegal chemicals.[33]

On February 24, 2000, the New York Police Department arrested a man for selling MDMA, GHB, ketamine, DXM (dextromethorphan), and more than 16 other substances over the Internet from Las Vegas. The sources for at least a portion of his drugs were several Chinese pharmaceutical companies. The man kept an extensive list of customers from almost every state, many of whom were minors, and his operations extended to nine countries. The New York Police Department also arrested a man in the summer of 2000 for selling MDMA over the Internet from Orlando. The individual was associated with shipments to 15 states. [34]

GHB

GHB was controlled as a Schedule I drug on February 18, 2000. Since that time, advertisements for GHB sales on the Internet have not been as common. Websites now are marketing GBL and 1,4-butanediol, GHB analogs that produce similar effects.[35] GBL and 1,4-butanediol sales are probably more common than those of MDMA or LSD. Sales of GHB still are arranged on the Internet; customers identify suppliers, place orders, and then receive GHB or GHB kits[36] in the mail for an agreed price.[37] Some suppliers sell GHB as a growth supplement,[38] and numerous websites advertising bodybuilding supplies and health supplements sell items containing GHB.[39]

Two brothers were recently sentenced to 4 years each for selling GHB "date rape" kits over the Internet to customers in New Jersey and other states. The brothers earned about $200,000 from sales that were made between March 1999 and January 2000.[40]

---

[31] San Diego Police Department interview, conducted by NDIC, 7 March 2001.
[32] "Internet Highway: Road to Enlightenment or Danger?" NDIC, 23 August 2000.
[33] *Trends In The Traffic, 1st Quarter 2001*, DEA Detroit Field Division.
[34] "Cops Chase Drug Dealers Hawking Wares On Web," *New York Daily News*, 20 July 2000, URL: <www.mapinc.org/drugnews/v00/n1017/a02.html?190661>; Las Vegas Metropolitan Police Department, email communication to NDIC, 8 March 2001; "Police Say Web Site Was Sham to Sell Drugs," Metro News Briefs: New York, URL: <http://english.peopledaily.com.cn/200007/18/eng20000718_45743.html>.
[35] *Trends In The Traffic, 1st Quarter 2001*, DEA Boston Field Division; *Trends In The Traffic, 1st Quarter 2001*, DEA St. Louis Field Division.
[36] GHB kits generally contain GBL and sodium or potassium hydroxide.
[37] "Field Intelligence Collection Plan," Fourth Quarter FY2000, DEA Miami Field Division.
[38] *Quarterly Trends In The Traffic Report, First Quarter FY 2001*, DEA Houston Field Division; "Field Intelligence Collection Plan," Fourth Quarter FY2000, DEA Miami Field Division.
[39] *Trends In The Traffic, 1st Quarter 2001*, DEA New Orleans Field Division.
[40] "Two brothers who sold 'date-rape' drug kits over Internet get prison," Associated Press, 23 March 2001.

A 45-year-old man was arrested in Las Vegas in March 1999 for selling GHB through a website and shipping it cross-country by mail. Law enforcement seized 200 gallons of chemicals, enough to produce a substantial volume of GHB worth more than $1 million at the street level.[41]

LSD

LSD advertisements are also uncommon on the Internet, given that LSD is a Schedule I controlled substance. However, as with the other "club drugs," sales are arranged through communications over the Internet. Information on the sale of LSD most often is seen on bulletin boards where customers and suppliers meet. Many LSD bulletin boards use a "frequently asked questions" (FAQ) structure; a moderator sets ground rules such as "never directly ask where to purchase LSD or share information regarding individuals who sell LSD." Website operators use such disclaimers to shield themselves from law enforcement scrutiny. Hallucinogens that approximate the effects of LSD and alternate sources for LSD production chemicals are advertised openly on the Internet.

In February 1999, a Louisiana state narcotics investigator arrested a 22-year-old woman and three of her friends after selling them fake LSD and MDMA tablets in an undercover operation. The sale, brokered in an Internet chat room, was extremely easy to arrange, according to the investigator.[42]

Newsgroup posting: "Does anyone sell ls*d in VA? I want large amounts….This is a stupid way of finding out but I can't find it anywhere in large amounts, raves, clubs, dealers, friends, etc. I'm too dumb to be a narc* PLease help me. I'll travel."[43]

Internet Sampling

NDIC conducted Internet searches to assess the availability of pro-drug information to the typical Internet user. NDIC used only conventional online search engines (Google, Northern Light, Yahoo, Alta Vista, and HotBot) and metasearch engines (Dogpile, Mamma, and C4). The goal was to find websites that promote or facilitate production, use, and sales of MDMA, GHB, or LSD. More specifically, NDIC searched for sites containing the information elements listed in Table 1.

[41] Jim Krane, "Narcs Online: Cops Chase Drugs Onto the Net," 22 September 1999, URL: <APBNews.com>.
[42] Jim Krane, "Internet Sting Greets Mardi Gras Revelers: Undercover Cop Nabs Four Accused LSD Buyers," 15 February 1999, URL: <APBNews.com>.
[43] URL: <alt.drugs.lsd> newsgroup, actual message posted at URL: <http://groups.google.com/groups?hl=en&lr…ic=1&th=67203b430183zbe9&seekd=986247431>, accessed on 12 April 2001.

Table 1. Drug-Related Information Elements on Offending Websites

PRODUCTION		USE		SALE	
Information on physical needs	*Instructions*	*General information*	*Information on use & co-use*	*Explicit sales*	*Implicit sales*
WHAT DO YOU NEED?	HOW DO YOU DO IT?	WHAT IS IT?	HOW DO YOU USE IT?	GET IT HERE	GET IT ELSEWHERE
Raw materials, equipment, personnel, production and storage facilities, packaging materials	Production processes, waste management, production tips and cautions	Descriptions, pharma-cology, analogs, studies and tests	Physical and psychological effects, best methods, risks and warning	Advertising, marketing, promoting, glamorizing; sales through electronic orders, charges, payments	Information on where to find or how to procure drugs and chemicals

NDIC identified 52 sites that contained at least one of these information elements as they pertain to MDMA, GHB, or LSD, demonstrating that "club drug" information is readily available to the typical Internet user. The 52 websites were examined further for content, with the following results:

Drug Activity

- 39 sites contained information on MDMA, GHB, or LSD use.
- 24 sites contained information on MDMA, GHB, or LSD production.
- 6 sites contained information on MDMA, GHB, or LSD sales.

Associations

- 35 sites contained links to other drug-related sites.
- 32 sites probably were associated with drug legalization groups.
- 10 sites were personal websites maintained by individuals.
- 10 sites probably were associated with businesses.
- 8 sites probably were associated with "party scene" or rave groups.

Law Enforcement Evasion

- 20 sites contained a "for information purposes only" disclaimer.
- 2 sites contained information on how to evade law enforcement efforts.

Seven sites targeted young people implicitly or explicitly. In general, sites maintained by pro-drug legalization groups did not specifically target young people, but websites dedicated to the party or club scene did target youth. Additionally, 14 sites provided connections to chat rooms or other interactivity tools.

Legal Issues: Challenges Facing Policymakers and Law Enforcement

The nature of the threat posed by pro-drug Internet websites raises a number of legal issues of which policymakers and law enforcement should be aware. The increasing popularity of the Internet has challenged legislators and law enforcement officials trying to prevent its use to facilitate drug crimes. Besides having to develop new investigative methods to adapt to computer technology, law enforcement agents must ensure that any new methods are constitutional and comply with federal statutes. Legislators trying to make certain that federal statutes effectively address the misuse of the new medium must do so without overreaching and violating individual rights. The following summarizes some of the legal issues that law enforcement agents and legislators may encounter. More information can be found in the *1997 Report on the Availability of Bombmaking Information* and in *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, both published by the Department of Justice.[44]

First Amendment, U.S. Constitution

Any government effort to restrict individuals from using the Internet to disseminate information that assists others in illegally producing, using, or distributing controlled substances must respect the First Amendment of the Constitution. The First Amendment strongly protects an individual's right to freedom of speech and can be infringed only in limited situations. Whether the government can prohibit an individual from disseminating such information over the Internet depends on factors such as the type of information disseminated, how it is disseminated, and the intent with which it is disseminated.

The *1997 Report on the Availability of Bombmaking Information* addresses a number of legal issues involved in limiting the dissemination of bombmaking information. Although the subject of the report was the dissemination of a different type of information, its legal analysis can be applied to the dissemination of information that facilitates drug crimes. The first issue to be discussed is whether the government can restrict the dissemination of information simply because it advocates the production, use, or distribution of controlled substances. This issue has been addressed by many courts including the U.S. Supreme Court, which clearly have ruled that any attempt to prohibit the dissemination of such information would violate First Amendment rights.

A second issue is whether the government can restrict the dissemination of lawfully obtained information that could be used by others to illegally manufacture, use, or distribute controlled substances. The answer to this issue is not as clear. However, courts often have held that if such public information is widely distributed to a large, unidentified audience, it cannot be restricted by the government without infringing on First Amendment rights. The rationale behind this decision is that even legitimate publications could be used to assist individuals to illegally manufacture, use, or distribute controlled substances. Legitimate publications might include textbooks on chemistry or agriculture, encyclopedias, or even government manuals.

By contrast, if the individual's dissemination of such information is directed towards a specific person or audience who acts on the information, the dissemination can rise to the level of "aiding

[44] These reports can be found at <http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html> and <http://www.cybercrime.gov/searchmanual.htm>.

and abetting" another in committing a crime. Such "aiding and abetting" is considered a "speech act" and is not constitutionally protected simply because it is speech. Whether an experienced methamphetamine producer provides an apprentice with face-to-face assistance or with help over the Internet, the instructions can still rise to the level of aiding and abetting a criminal act. Such activity is not protected by the Constitution because, unlike disseminating information to a wide audience that may or may not engage in the illegal activity, this dissemination is directed at a person or persons to assist in committing illegal activity. Even if the recipients of the information act upon it at some later date, the disseminator can still be prosecuted.

A closely related issue is whether the government can prohibit an individual from disseminating information with the *intent* of assisting another person in the illegal manufacture, use, or distribution of controlled substances, even when the recipient does not actually act on the information. The Department of Justice has referred to this issue as "attempted aiding and abetting." Court decisions seem to allow prohibition of such dissemination if the government can prove that the individual disseminated the information with the *specific intent* of assisting another individual in committing a drug crime. Individuals prosecuted in cases with similar issues have argued that they did not know how the recipients were going to use the information and that they provided the information for legitimate purposes, such as scientific research, law enforcement purposes, or general public interest. However, prosecutors have been able to prove intent in some situations by showing that the disseminated information contained declarations demonstrating a purpose to facilitate drug crimes, or that the disseminated information had no use other than to facilitate drug crimes.

Another closely related issue is whether the government can constitutionally prosecute individuals who disseminate information with the *knowledge* that a specific recipient intends to use it to illegally manufacture, use, or distribute a controlled substance. Whether such a restriction is valid under the Constitution is not clear. According to analysis in the Department of Justice's bombmaking report, such a prosecution would probably survive a constitutional challenge as long as the government was required to prove that the individual had reasonable cause to know that a specific recipient of the information intended to use the information to commit a crime.

Jurisdiction

The Internet has allowed individuals to conduct real-time criminal activity without regard to geographic boundaries. Law enforcement officers investigating such activity must determine the actual location of the criminal activity and then what legal requirements apply to that jurisdiction.

Criminal activity conducted over the Internet from a foreign country is just one situation that can cause jurisdictional problems for law enforcement officers. The Internet allows individuals located in a foreign country to induce criminal activity in the United States; however, since the individuals are actually outside the country, they are often untouchable by the U.S. government. Even if a foreign government assists U.S. law enforcement officers in the investigation, the investigating officers must comply with sensitive and complex international policies.

Individuals conducting criminal activity from within the United States can also cause jurisdictional problems for investigating officers. Individuals committing crimes over the Internet can be located in various geographical locations, and the computers storing the data can be in places separate from the individuals. Prosecution can be difficult because the locations often cross over different judicial districts, and that can affect various legal procedures. For example, when investigators apply for a search warrant to obtain data stored on a computer, they must consider the judicial districts in which the evidence is actually stored. Although an agent might be accessing information while he is in New Jersey, the data could be stored in another judicial district in the United States. This situation sometimes requires investigators to obtain multiple warrants from different judicial districts.

Privacy Statutes

Searches of computers by law enforcement officers attempting to gather evidence of crimes committed over the Internet must comply with federal statutes that protect individual privacy. Two major statutes are the Privacy Protection Act (PPA), 42 U.S.C. § 2000aa, and the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701-2730. If officers performing searches of computers fail to abide by these statutes, they risk civil liability for their actions.

The PPA affects law enforcement officers investigating crimes committed over the Internet because it generally prohibits them from seizing materials that are possessed for the purpose of publishing information to the public. A person using a computer to post information on the Internet may be considered a publisher under the PPA.

An exception under the PPA permits law enforcement officers to seize materials that are contraband or evidence of a crime. However, this exception does not give officers carte blanche to seize all the data on the computer, and officers may have difficulty separating information that is contraband or evidence of a crime from information not connected with the investigation. For example, if a computer is used to publish a website that assists other individuals to commit drug crimes and the same computer is used to publish a website that addresses politics, the information connected with the drug crime website would not be protected under the PPA, but the information connected with the political website could be protected under the PPA. A mistake by the officers could expose their agency to liability.

Another statute, the ECPA, is aimed at protecting the privacy of electronic communications. To comply with the ECPA, law enforcement officers must take special precautions when searching or seizing computers that contain electronic communications from third parties. These precautions are especially important when gathering evidence from an ISP. Like the PPA, the ECPA imposes civil liability on agencies for any violations of the Act.

Both the PPA and the ECPA are complicated bodies of law. Individuals wanting more information may wish to read *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.

Execution of Warrants

Because data can be erased easily from computer systems, investigators executing search warrants must consider the possibility that individuals may try to destroy evidence before it can be seized. Individuals can set up their computers so that typing a few keystrokes will initiate the rapid destruction of incriminating files. Also, data can be stored in various geographical locations, and any number of persons with access to the information can destroy it even while investigators are executing a search warrant. To avoid the loss of important evidence, investigating officers may want to take extra precautions, such as conducting no-knock searches.

Evidentiary Issues

Proving a criminal case in court that involves computer records creates certain evidentiary challenges. For instance, in order to use computer records as evidence in court, the government must establish that they are "authentic" or are what they appear to be, and authentication of computer records can be difficult. Computer records can be changed easily, and defendants sometimes claim that records were altered after they were created. Computer errors can result in mistakes in the data as well. Also, the identity of the author of the records can be difficult to establish. Unlike handwritten material, computer records do not have a distinctive style, and so other evidence must be used to establish authorship.

Project Continuation

In phase two of this project, NDIC will produce a full strategic assessment of the Internet drug threat. NDIC will coordinate with DEA and other federal law enforcement agencies as appropriate. The assessment will address in greater detail the intelligence requirements on the production, use, and sale of illegal drugs by concentrating on the following issues:

1. Identifying the federally scheduled, nonprescription drugs and drug paraphernalia that constitute the problem.
2. Estimating the number of websites and providing an estimated breakdown by drug type, by activity type, and possibly by level of activity (high, medium, low).
3. Identifying the locations of website domains and the locations of routers for servers hosting websites (specific locations and/or general observations).
4. Assessing the ability of law enforcement to physically locate individuals/groups.
5. Describing organizational affiliations (organizations/groups/gangs/independent entrepreneurs, ethnic/demographic composition, regional/national/international, etc.).
6. Describing the methods of operation individuals/groups use to conduct business and evade law enforcement (processes, tactics, technical sophistication, creation/secretion/movement of websites, deception/countermeasures, security, legal considerations, etc.). Describing how the Internet's size, traffic, capabilities, audience, etc., affect methods of operation. If drug organizations account for part of the threat, describing their operational infrastructure (key functions, command and control, inter- and intraorganizational relationships).